

Children's Charities' Coalition on Internet Safety

Digital manifesto

John Carr
Dr Zoë Hilton



as long as it takes



Contents

Why a digital manifesto?	2
The internet, children and young people – an overview	3
Summary of recommendations	4
Section 1: The growth of the internet	10
Section 2: Summary of children’s vulnerability	14
Section 3: Government and stakeholder responses	23
Section 4: Child abuse images	28
Section 5: Part 1: New and emerging issues	38
Part 2: Ongoing concerns	46
Section 6: Self-regulation	51

as long as it takes

Why a digital manifesto?

With a general election approaching, the Children's Charities' Coalition on Internet Safety (CHIS)¹ has prepared this 'digital manifesto', which it is sending to all the major political parties.

CHIS asks the parties to commit themselves to supporting the policies and recommendations it contains. Details of the responses received will be published.

In her report for the Prime Minister published last year,² Professor Tanya Byron addressed many of the challenges surrounding children and young people's use of the internet and other new technologies. Byron provided an ambitious plan of action which, if fully implemented, will deliver many tangible benefits.

More than 12 months after publication of *Safer Children in a Digital World*, this manifesto updates aspects of it but it is also intended to help guide the work on implementation that is now underway.

¹ The members of CHIS are Action for Children, The Children's Society, ECPAT UK, NCB, Children England, NSPCC, Stop It Now UK and Ireland.

² *Safer Children in a Digital World* (The Byron Review), DCSF, March 2008

In addition, the digital manifesto discusses a number of issues that were outside the scope of the Byron Report but are nonetheless very important to children and young people's safety online, such as the treatment of child sex offenders and aspects of policing.

There is no doubt that in the five years since the last manifesto was published, the various interests concerned with keeping children and young people safe on the internet have achieved a great deal. UK-based internet and mobile phone companies, child protection and law enforcement agencies, the academic and research communities, and the UK Government have become acknowledged leaders in the field globally. And yet, much still needs to be done, some of it urgently. This manifesto points the way.

John Carr, Secretary of CHIS

Dr Zoë Hilton, Policy Adviser on Child Protection to the NSPCC

There is no doubt that in the five years since the last manifesto was published, the various interests concerned with keeping children and young people safe on the internet have achieved a great deal.

The internet, children and young people – an overview

The internet³ has become an enormously important technology in the modern world. Many different societies, on all continents, are benefiting from its development. CHIS strongly believes in the potential of the internet to enrich the lives of children and young people. The internet's ability to provide a platform for games, connectivity and creativity is also an undoubted part of its value and its attraction to hundreds of millions of children and young people worldwide. CHIS actively promotes safe and equal access to the benefits of the internet to all children and young people.

However, the internet can also expose children and young people to harm, for example by exposing them to age-inappropriate material or illegal content, or indeed to sexual predators or bullies.⁴

³ There are many ways the internet can be accessed, eg via laptop, desktop, notebook-sized or handheld computers, through mobile phones, games consoles, personal digital assistants and TV. Rather than repeat this list throughout this document, unless the text provides otherwise, all of these routes are relevant.

⁴ See below pg 15 et seq for a fuller description of potential harms.

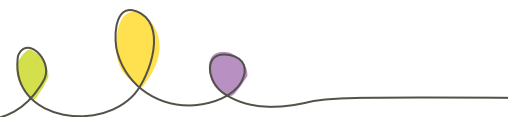
Children and young people have a right⁵ to grow up and develop in a safe environment that is free from sexual or other kinds of exploitation. They need to be equipped to keep themselves safe online. Parents and guardians should be helped to understand how children and young people use the new technologies so they, in turn, can help ensure not only that children and young people get the most out of the technologies, but also that they know how to use them safely. Schools and the internet industry have vital supporting roles to play here and the voluntary sector is also a key player.

No one company or single agency has a monopoly of knowledge or expertise. Providing a safe environment on the internet for children and young people is a shared responsibility, just as it is a shared responsibility in any other environment.

⁵ Conferred by the UN Convention on the Rights of the Child and these protections are enshrined in UK domestic legislation, eg Children Acts 1989, 2004



Summary of recommendations



All of the following recommendations also appear in the main body of the manifesto as italicised text.

Child abuse images⁶

1. The Government should prepare a Bill that will compel all internet service providers (ISPs) based in the UK to adopt the Internet Watch Foundation (IWF) list, or some other technical solution that blocks access to all known child abuse websites and newsgroups. The Bill should also detail or make provisions for a method by which compliance with this policy can be tested and publicly confirmed. If it becomes clear that some ISPs will refuse to implement a blocking solution unless compelled to do so by law, the Government should immediately put the Bill before Parliament.
2. In the meantime, an instruction should be issued to all Government departments forbidding them from purchasing internet services from any ISP that does not deploy a solution that blocks access to all known child abuse websites. The Government should also encourage the remainder of the public sector to follow its lead.
3. The IWF should consider adopting new or additional methods to speed up take down times for child abuse images hosted overseas.
4. The Government should promote discussions at an international level with a view to improving substantially the speed with which, once notified to the relevant authorities overseas, child abuse images on the internet are removed altogether or access to them is denied.
5. The Government should consider the use of tax or other incentives to encourage ISPs and technology companies to develop and deploy new or speedier ways of tracking, blocking or destroying online child abuse images.
6. The Government, law enforcement and the industry should begin discussions about how to combat the use of peer-to-peer software for the distribution of child abuse images and about how to combat the emergence of other types of closed groups or communities that have the same purpose. An immediate start could be made by looking to the industry to fund a specific, time-limited operation similar to that deployed by the music and film industries to protect their copyrighted material from unlawful exploitation by file-sharing software.
7. The high-tech industries should urgently address ways to prevent the misuse of anonymity, encryption software and other technologies from facilitating the exchange of child abuse images.
8. The Financial Services Authority should take a close look at the way pre-paid card systems, particularly those that can be obtained and used anonymously, might be fuelling a growth in criminal exchanges on the internet, particularly around child abuse images.
9. In order to promote the more efficient blocking of child abuse websites worldwide, the UK Government should engage with the EU and others with a view to expediting the creation of a single list of all known child abuse websites, or a list that is as large as possible, drawing on any and all national lists that are not

⁶ The term 'child abuse images' is used throughout this document to denote pictures or videos that are illegal under s.1 Protection of Children Act, 1978, as amended by s.84 Criminal Justice and Public Order Act, 1994 and s.41(1) Criminal Justice and Court Services Act, 2000, and s.160 Criminal Justice Act, 1988, as amended by ss.84(4) and 86(1) Criminal Justice and Public Order Act, 1994. Such images are otherwise referred to as indecent images of children, or historically as child pornography. This change in terminology reflects a growing awareness of the nature of the content typically found in these images and videos.



encumbered by local legal constraints. With appropriate security surrounding its deployment, this resource should be made available to relevant online service providers, filtering companies and others with an appropriate interest in blocking access to or investigating websites containing child abuse images.

10. The Government should play an active role in promoting the greater harmonisation of national laws and police procedures for dealing with online child abuse images. In particular, the Government should sponsor the development of an internationally based investigative unit with a specific remit to focus on the criminal networks behind a very high proportion of the trade in child abuse images.
11. The Government should promote discussions at an international level to find ways of preventing the trade in or hosting of child abuse images moving to countries with poorly developed laws on cyber crime or few resources locally to enforce such laws. In addition, the Government, the EU and others should make representations to the Internet Corporation for Assigned Names and Numbers (ICANN) with a view to securing a substantial improvement in the regulatory performance of those individual domain name registries that currently appear to be ineffective in preventing child abuse images from being published under their auspices.
13. The Government should fund more research into the long-term consequences for, and therapeutic needs of, children who have been sexually abused where images of that abuse have appeared on the internet. The Government should also ensure appropriate resources are developed to address these needs and that the children's workforce is trained to identify them and knows how and where to refer children in order to ensure they receive appropriate support.
14. Drawing on the technical research currently being funded by the EU's Safer Internet Programme and others, the Government should provide more resources to help law enforcement to achieve a higher rate of detection and location in real life of children who have appeared in child abuse images on the internet.

Other research and information needs

Child abuse images – research

12. Large-scale research is needed to determine whether or to what extent there is a link between the offence of possessing child abuse images and committing other types of sexual offences against children. Research should also seek to establish if the possession of different types of child abuse images can be used as a predictor of likely future risk to children.
15. The UK Council for Child Internet Safety (UKCCIS) research programme should give priority to determining overall prevalence levels for different types of risks to children online and to determining the extent to which a range of factors render children and young people more or less vulnerable to such risks.
16. In order to inform future design and implementation, it is important that there is a full and independent research-based evaluation of current education and awareness programmes to determine what approaches are most effective.
17. It is important that we develop a better understanding of the range and spectrum of children's sexual behaviours online and develop a better understanding of how to assess and treat harmful sexual behaviours that are manifested in the online environment.



Policing priorities

18. The Home Secretary should make child protection a statutory performance indicator that is reflected in the priorities of every local police force in England and Wales and an equivalent measure ought to be adopted in Scotland and Northern Ireland.
19. The Child Exploitation and Online Protection Centre's (CEOP) core funding ought to be sufficient to cover all of their operational needs and should not leave them dependent on external agencies to resource any significant areas of their work.
20. Law enforcement agencies should be required to record all instances where the internet or new technology played a significant role in sexual abuse or other crimes involving children. This information should be recorded centrally by the Home Office. The data should include information about the age and any other relevant characteristics of the victims and the perpetrators. It should also be published broken down by reference to the constabulary area where the crime was committed.
21. Additional resources are urgently required to enable the police or other investigating authorities to improve the speed with which they can conduct forensic and other examinations of digital devices that are part of a criminal investigation into child abuse.

Access to age-restricted goods and services and data protection

22. Legislation should be brought forward to provide for the development of regulations governing the online sale of age-restricted goods and services.

23. The Information Commissioner's Office (ICO) should issue clear, research-based advice and guidance on the respective rights and responsibilities of all the parties where online data transactions involving legal minors are concerned. In particular, the ICO should consider setting (or asking Parliament to set) a legally defined minimum age below which verifiable parental consent will always be required in an online environment.

Addressing future challenges of the mobile internet

24. Major providers of wifi access should replicate the arrangements currently made by the mobile phone companies for restricting access to adult sites on the internet.
25. The mobile phone handset manufacturers should accept a larger role in the ongoing discussions about child safety on the internet with a view to developing safety features that can operate by default and are integrated directly into the handsets.
26. Mobile phone handset manufacturers and network providers should consider developing devices for children that have a much-reduced feature set and therefore avoid some of the risks that seem to be unavoidably associated with the more sophisticated models.
27. The Government should initiate an inquiry into the new location technologies now emerging into the mass consumer market that, typically, centre on or use mobile phone handsets. The inquiry should recommend what steps need to be taken both to ensure that such services are marketed responsibly and to ensure that adequate security safeguards are in place to protect children and young people.



Advertising to children

28. A clear definition of what constitutes a children's website should be formulated and all advertising on such sites must conform to the Advertising Standard's Authority's Code of Advertising, Sales Promotion and Direct Marketing (CAP code).

Internet safety software

29. The Government should announce that within the next 12 months it intends to begin a review of progress on the take up and use of child safety software in the consumer market in respect of all internet-enabled devices.
30. The Government should consider providing incentives for firms to develop new technical measures that are designed to help protect children and young people online.

Support for professionals

31. The professional bodies responsible for the accreditation of police, health, probation, prison staff, social workers, youth workers and teachers need to ensure that proper recognition is given within their professional qualifications and their professional development programmes to the importance of dealing appropriately with online offending or other related problematic behaviours.
32. The social work professions, youth workers, health service personnel and others who engage with children and young people more generally need to become more closely engaged in the analysis of risks to children and young people on the internet and in the discussions about how best to provide some of the solutions. In particular, these groups need to be familiar with both the

manifestations of online abuse in victims, and of the kinds of abuse engaged in by perpetrators.

33. Appropriate advice should be available to all parts of the judiciary in relation to the nature and impact of the different types of online offending against children and young people.

Treatment provision

34. The Ministry of Justice, the Home Office, the Department of Health and other relevant agencies need to ensure that there is sufficient availability and take up of treatment programmes for internet offenders. They also need to ensure that police and probation officers are appropriately trained to manage the risks posed by internet offenders, thereby minimising or reducing the prospect of them re-offending or otherwise putting children in jeopardy.
35. Appropriate assessment and treatment should be available for children displaying inappropriate or aggressive sexual behaviour online.

Social networking sites

36. Social networking sites should ensure they meet all the recommendations of the Home Office good practice guidance for the providers of social networking and other interactive services, giving urgent attention to their procedures for reporting abuse.
37. Social networking sites should ensure they have a mechanism that allows them to review content on their site, especially pictures and videos, and also ensure that they review all content reported to them within a clearly specified time period.

38. UKCCIS should give a high priority to the development of an independent mechanism for determining compliance with the recommendations of the Home Office good practice guidance for the providers of social networking and other interactive services.

Removing legal barriers

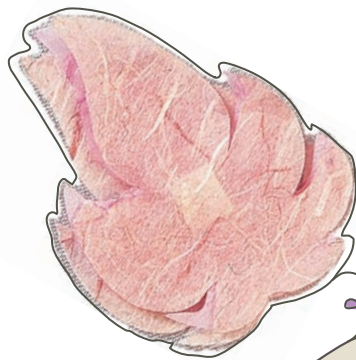
39. Efforts should be made to clarify the civil and criminal liabilities of ISPs and other online service providers in relation to user-generated content hosted on their websites. In particular, the Government should press for an amendment to the E-Commerce Directive to remove any disincentive for internet companies to police their own sites for fear of attracting liability. ISPs and other online hosting companies should not lose the protection of ‘mere conduit’ status simply because they tried to locate and remove inappropriate or illegal content. The principle should be that for liability to exist it is necessary to show an ISP or hosting company had actual knowledge of the illegal content and deliberately took no action or failed to act within a reasonable time.

Future progress and policy development on internet safety

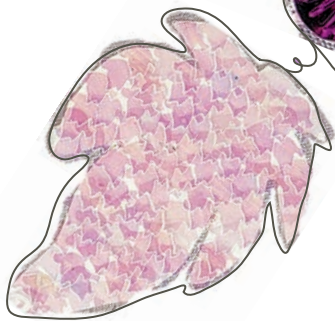
40. The Government and law enforcement should seek to reduce their dependency on the internet and high-tech industries by developing their own independent sources of technical knowledge and expertise in these highly complex areas.
41. The Government should find ways to help the third sector to develop its own capacity to engage constructively and in a well-informed way, both nationally and internationally, with the consultative and other processes that are central to the development of policy in this area.
42. For public confidence in self-regulation to be sustained, the model must be seen to work effectively. More energetic and visionary leadership from the high-tech industries is required.







Section 1



as long as it takes

Section 1

The growth of the internet

Setting the scene – rapid growth presents challenges

The internet is still barely 15 years old as a consumer-facing technology.⁷ Within that 15 years, the internet has gone through many iterations, and the signs are that the rate of change will continue apace, presenting a constant series of new challenges to children and families, policy makers, governments, legislators, law enforcement, regulators and the industry itself.

In the first quarter of 1999, only 3.2 million UK households had an internet connection. This then represented 13% of all households. By the end of 2000, this had gone up to 8.6 million, or about 33%.⁸ Today it stands at 16.5 million households, of which approximately 13.5 million have a broadband connection⁹ (this represents 65% of all households).

In May 2001, the Government released the first set of statistics showing the then level of e-commerce. Based on a survey of 9,000 businesses with 10 or more employees, they estimated that nearly £57 billion of sales were made online. This represented 2% of total sales for the sectors surveyed.¹⁰ In 2007, internet sales by UK businesses had risen to £163 billion, which, in turn, represented a 30% increase on the previous year.¹¹ By 2012, '£1 in every £5 of all new commerce' will be online.¹² In 2006, for the first time ever, the amount of money spent on advertising online exceeded the amount spent on advertising in newspapers.¹³ Today, in the midst of a recession, spending on online advertising is still set to grow, if only modestly, whereas spending on advertising in the more traditional media will continue falling.¹⁴

'Convergence' is the buzzword: companies supplying mobile phones, TV, broadband and landlines are increasingly merging or partnering with each other to provide a 'quad play' package. Almost all new games consoles are internet enabled. Once IPv6 (Internet Protocol version 6) is fully rolled out, every household appliance in the UK could be connected and the signs are that many of them will be.¹⁵

Old problems in new guises

One of the most striking features of this digital manifesto, as compared to the one CHIS published before the general election in 2005, is both how little some of the underlying issues have changed but also how much the presentation and manifestations of those issues have altered.

In the 2005 manifesto, the reader will find no reference to 'social networking', a phenomenon that emerged from nowhere and came to dominate the online child safety agenda in the space of three years. Similarly, while in the previous manifesto CHIS highlighted the importance of age verification in relation to the online sale of age-restricted goods and services, the later emergence of pre-paid credit cards¹⁶ has added greatly to the sense of urgency now surrounding that topic.

The nature of the internet is such that new manifestations of old problems arise all the time. Some of the risks now identified with social networking sites are the same as those that had been around for several years and had presented themselves in blogs, bulletin boards, chat rooms and instant messaging. The qualitatively new aspect that is the hallmark of social networking sites is the way

7 For a fuller account of the history of the internet, see www.isoc.org/internet/history

8 www.statistics.gov.uk/pdffdir/intacco702.pdf

9 www.statistics.gov.uk/cci/nugget.asp?id=8

10 Ibid

11 *Digital Britain*, BERR, HMSO, January 2009, p3

12 <http://news.bbc.co.uk/1/hi/business/6502773.stm>

13 <http://news.bbc.co.uk/1/hi/business/6502773.stm>

14 www.endersanalysis.com/publications/publication.aspx?id=652

15 Although to what end is not always very clear.

16 Or 'stored value cards', to give them the name preferred by the financial services industry. Since many of these cards display the Visa and Mastercard logos, they seem destined to be called 'credit cards' by the average consumer, at least for the foreseeable future.

they brought these pre-existing technologies together into a single place, added new features, and created very user-friendly interfaces. This made it simple for people to personalise their own web pages. They could add examples of their favourite music, photographs and videos. Together these made up and became an important extension of the author, a way for someone to make a statement about themselves. This triggered the astonishing growth in the popularity of social networking sites, which caught many people by surprise.

Virtual and real worlds becoming more closely aligned

As children and adults increasingly live out important parts of their lives with and through the new technologies, the nature of the risks they take have become inextricably entangled with wider aspects of their behaviours. If it ever was, it is now simply no longer possible to draw neat lines between so called ‘internet issues’ and ‘real world’ problems. A tightly maintained consensus within the policy community about some of the earlier problems that were identified with the internet around, for example, child abuse images and the grooming of children by sex offenders, has now given way to a range of debates about how children ought to be encouraged to behave online. These new debates touch on wider issues, for example at what age is it acceptable to allow children to be exposed to different kinds of material, whether on the internet or elsewhere, and what exactly constitutes ‘normal’ risk taking, online as well as off? Questions have even been raised about how the new technologies might be affecting the development of children’s brains or adversely affecting their ability to concentrate.¹⁷ With this widening of

¹⁷ ‘...the mid-21st century mind might almost be infantilised, characterised by short attention spans, sensationalism, inability to empathise and a shaky sense of identity’, Baroness Professor Susan Greenfield, House of Lords, Hansard, 12 February 2009.

the parameters of internet safety debates, the difficulty of reaching or maintaining a consensus has increased.

Digital divide?

In recent years, and partly to counter some of the criticisms about the impact of new technology, one of the dominant narratives that has emerged in the digital space is about how the internet is a liberating tool for children. A great deal of money and power has been put behind the promotion of that idea. Yet for some children and young people, the internet clearly fails to deliver on this promise and, even leaving aside questions of risk, they may have a narrow and unrewarding internet experience.

The internet certainly can provide an enormously enriched environment across a very broad range of educational, social and economic activities for very many users, particularly younger users. However, the arrival of the internet could also be contributing to a further widening of pre-existing divisions in society or even be responsible for opening up new ones.¹⁸ It is a divide rooted not only in possessing, or not possessing, the physical means of accessing the internet; it is a divide that is influenced by many other factors.¹⁹

Professor Sonia Livingstone’s research into children and young people’s activities online identified a digital divide not only in terms of having physical access to the internet but also in terms of different levels of experience.²⁰ An individual’s level of media literacy and self-confidence in using the internet will be

¹⁸ Similar points have also been made, particularly at the UN, about how at a macro level a new social and economic divide can open up between countries that have, or do not have, large-scale access to the new technologies.

¹⁹ In *Delivering Digital Inclusion: An Action Plan for Consultation*, HMSO, October 2008, the Government identified a potentially increasing depth of exclusion for those who are not using the internet in terms of a higher cost of living, a lack of access to services and loss of employment opportunities. (see www.itu.int/wsis/docs/geneva/official/dopghtml)

²⁰ *Drawing conclusions from new media research: reflections and puzzles regarding children’s experience of the internet*, LSE, 2006

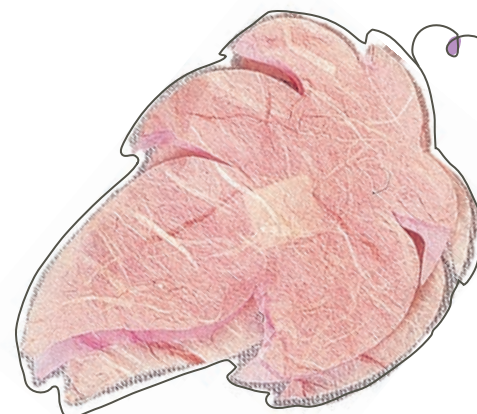
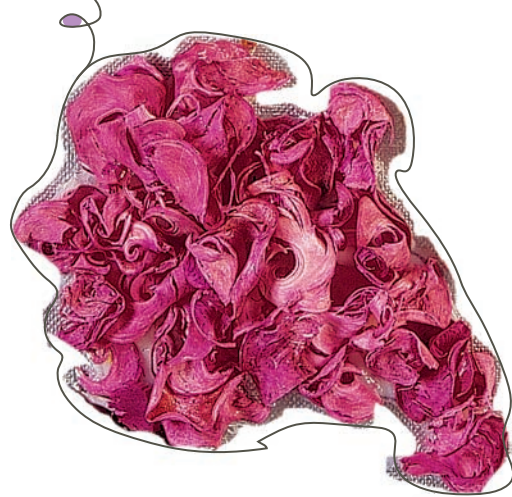
decisive in determining whether or to what extent that individual benefits from it. If this is not addressed, there is a very real danger that more socially excluded children will have a poorer internet experience when they go online. For these reasons, CHIS very much welcomes the current emphasis in Government policy on bridging the digital divide not only in relation to improving access²¹ but also in relation to improving the media literacy and self-confidence of users. Much will depend on the successful delivery of policies that address this aspect.

Risk and harm

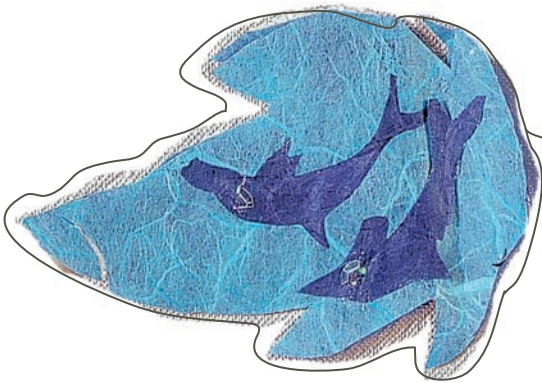
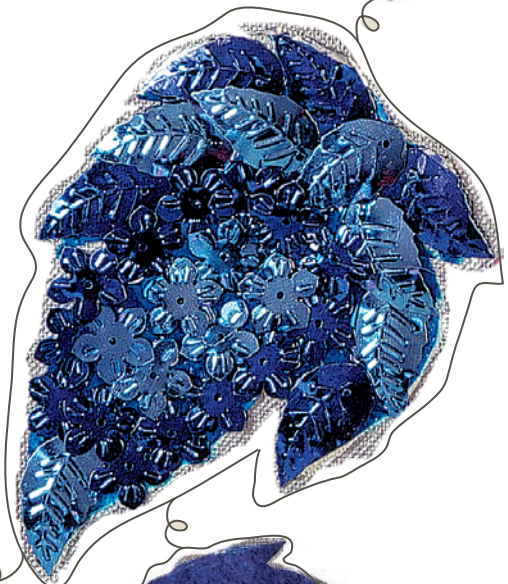
Then there is the question of risk and harm.²² There is no doubt that the arrival of the internet has introduced new risks to children and young people and that these carry with them the potential for significant harm. However, in the UK, the different experiences and vulnerabilities of a broad spectrum of children and young people active in the online space have not been well explored. When discussing how to approach issues of internet safety, the focus is often on how the safety messages or educational programmes would be received by or work with a notional or idealised family and a notional or idealised child. Such responses overlook the needs of a great many children and families who do not fit that model.

²¹ See www.dcsf.gov.uk/pns/DisplayPN.cgi?pn_id=2008_0208

²² This is discussed more fully below at pg 15 et seq



Section 2



as long as it takes

Section 2

Summary of children's vulnerability

Risks to children on the internet

While adults and children alike are exposed to a range of risks and dangers online, children and young people in general are often particularly vulnerable. As Professor Byron explained in detail in her review,²³ children are still in a process of developing and learning, which has consequences for their capacity to identify, assess and manage potential risks. The idea that children are vulnerable and should be protected from all forms of exploitation is outlined in the UN Convention on the Rights of the Child.²⁴ As a coalition of children's charities, the principle that children are vulnerable and that their welfare should be protected and promoted is core to our perspective and our work on internet safety. It is also embedded in the entire range of policies and legislation underpinning the social care of children, including the 'Every Child Matters' agenda and the Children Acts of 1989 and 2004.

There are a number of issues about children and young people's use of the internet that are of ongoing concern to parents and children alike, as well as to governments, politicians and the policy-making community. These concerns may be summarised as follows:

²³ Op cit. Byron Review, pg 30

²⁴ www.unhcr.ch/html/menu3/b/k2crc.htm
The UK is a signatory to this treaty

Content

1. The internet's ability to expose children and young people to legal but age-inappropriate material, eg adult pornography or very violent imagery.
2. The internet's ability to expose children and young people to illegal content, eg child abuse images.

Contact

3. The internet's ability to expose children and young people to sexual predators, be they adults or other minors.
4. The way in which the internet may expose children to harmful online communities such as sites that encourage anorexia, self-harm or suicide, as well as sources of political influence espousing violence, hate and political extremism.

Conduct

5. The way in which the internet facilitates and can promote risky sexual interactions between children, including encouraging them to take and post pictures of themselves or others (eg 'sexting') that, aside from being harmful, may also be illegal.
6. The way in which some aspects of the internet encourage children to place in the public domain information about themselves, or post pictures or videos or texts, that might compromise their personal safety or jeopardise a number of career options in the future.
7. The internet's ability to expose children and young people to bullying and to allow or promote an environment in which children and young people are encouraged to bully others.

Commerce

8. The ways in which the internet has enabled children to access or acquire age-inappropriate goods and services, typically goods and services that they could not obtain on the high street.
9. The internet's ability to expose children and young people to scams, identity theft, fraud and similar threats that are economic in nature or are rooted in inadequate or unclear data protection or privacy laws.

Addiction

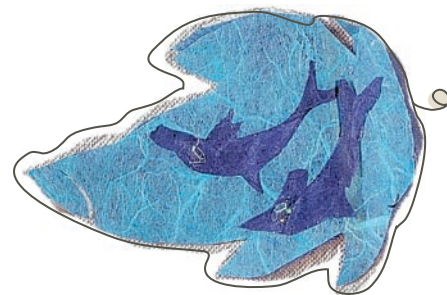
10. The way the internet seems to have encouraged, with some children and young people, forms of obsessive behaviour or excessive use that may be having a deleterious effect on children and young people's health or social skills, or both.

Societal

11. The way the internet has opened up a new digital divide among children and young people, both in terms of those who have ready and convenient access to it at home, school and elsewhere, and those who do not, and between those who are confident and proficient users of it and those who are not. This divide threatens to entrench or widen existing patterns of advantage and disadvantage or perhaps create new divides.
12. The potential of the internet to compound and even magnify the existing vulnerabilities of particular children and young people and add to adversities that they may face in the offline world.

Evidence of risk and harm

Tanya Byron commissioned Professor David Buckingham to undertake a board overview of the research literature concerned with the impact of the media on children and young people. Buckingham looked at the available evidence on bullying and exposure to certain kinds of content but, in common with the Byron Review itself, it did not look in any depth at many of the issues covered elsewhere in this manifesto. A large part of its findings related either to computer games or to wider issues of media literacy.



Bullying

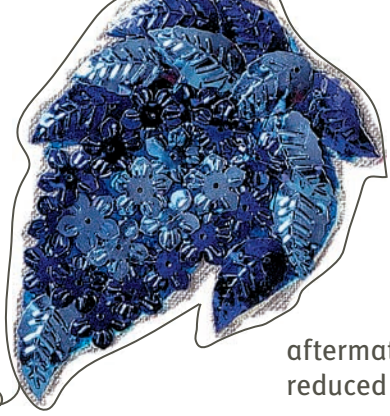
The most prevalent form of problematic behaviour online that children and young people have to face is bullying, with one in five children saying they have experienced it.²⁵ Bullying will affect children differently, but we know that for some the consequences can be deeply harmful, leading to self-harm or even suicide. The very scale of bullying online indicates that dealing with it must remain a core concern for all online education initiatives and related safety strategies. Several NGOs and other organisations have done a lot of work around online bullying and there are now some excellent resources available to help address the issues raised.²⁶

Child abuse images

Offences involving child abuse images continue at levels that were unimaginable prior to the arrival of the internet. The number of persons proceeded against or cautioned has fallen from the historic highs witnessed in the

²⁵ Action for Children found that 20%–25% of school students had been cyber bullied (*Putting U in the picture. Mobile bullying survey 2005*, NCH, see www.filemaker.co.uk/educationcentre/downloads/articles/Mobile_bullying_report.pdf), compared with 22% in a study completed by the Anti-Bullying Alliance in 2005 (see www.anti-bullyingalliance.org).

²⁶ See www.antibullyingalliance.org for further information.



aftermath of Operation Ore,²⁷ but they have not reduced as dramatically as expected.

In the UK, from 1988 until 1995 inclusive, the number of persons proceeded against or cautioned for offences relating to the taking, making or possession of child abuse images was steadily increasing but the average number per year was still under 100.²⁸ In 1996, the internet boom really started to take off in Britain, and in that year 236 persons were proceeded against or cautioned for offences relating to child abuse images. In 2003, in the aftermath of Operation Ore, this total peaked at 2,234. In 2007, the latest year for which figures are available at the time of writing, the number dropped back to 1,402. This fall surprised many commentators who had believed that the post-Ore reduction would be much larger. These figures indicate that significant numbers of people in the UK retain an interest in child abuse images. This suggests that while Operation Ore was a uniquely large police action, there remains a need to maintain a high level of police engagement with this type of offending. Similarly other measures to counter the trade in these images need to be improved.²⁹

Contact offending

Much of the public discussion about online risk or harm to children in the UK has focused on the most serious and widely publicised form of harm: sexual abuse. Yet even here the overall picture is unclear. In the early days of the internet every new case of child abuse online received national media coverage, and it was therefore possible to maintain some sort of overview of the scale of this type of offending. This no longer occurs. Generally these stories now only get reported if there is something new or unusual about the case.

²⁷ Operation Ore began in 2001 following receipt of a list from the US authorities containing over 7,000 names of UK residents who, using credit cards, appeared to have bought child abuse images from a Texan website.

²⁸ Offending and Criminal Justice Group (RDS), Home Office, Ref IOS 503-03

²⁹ This is discussed in more detail below at pg 29 et seq.

The true picture of internet-related crimes against children in the UK is in fact quite hidden. In part this is because the Home Office does not require the police to record where new technologies have played a role in sexual abuse cases involving children and young people.³⁰

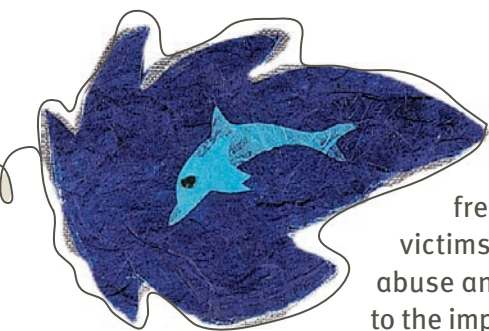
Internet Safety Technical Taskforce report

On 31 December 2008, the Berkman Center of Harvard University published *Enhancing Child Safety and Online Technologies*. It was the product of nearly a year's deliberations by the Internet Safety Technical Taskforce (ISTTF), with a specific focus on social networking sites. The extensive literature review published as Appendix C³¹ appears to suggest that the children who were at risk on the internet were the same children who were also at risk in the real world because of problematic family backgrounds or poor parenting. The report focused almost entirely on evidence drawn from US studies, and while it is extremely important for UK practitioners to be aware of it, its findings in this regard cannot be accepted as being conclusive in relation to the situation in the UK.

Anecdotal but persistent reports from UK police forces are quite clear that a large proportion of young people whom they are coming across, both as victims of various kinds of online abuse and as perpetrators of it, are not from vulnerable or other groups with whom they traditionally have a great deal of contact. Many of the children and young people they are dealing with in relation to internet-related matters come from families that have previously had little or no contact with social services or the police. While it may well be the case that children from more socially excluded and vulnerable groups

³⁰ The same is also true for many other types of offence.

³¹ <http://cyber.law.harvard.edu/research/isttf>



frequently are victims of online abuse and vulnerable to the impact of internet risks, there is no doubt that other children can also become victims.

Perhaps this apparent difference between the USA and the UK is rooted principally in differences in the demographics of internet usage, or alternatively it may be explained by reference to differences in the way in which risk is identified or reported either to social services or to the police, or both, in each country. What this discussion also highlights, at least in the UK, is the need for the social work professions and those who work with young people more generally to become more closely engaged in the analysis and the debate, perhaps also in providing some of the solutions.

The ISTTF study suggests that the scale of contact offending arising from online contacts has been exaggerated, citing one survey in which only 'two youths out of 1,500 (one 15-year-old girl and one 16-year-old girl) surveyed reported an offline sexual assault which had resulted from online solicitation'.³² According to the ISTTF, often the victims of sexual abuse that began online, while undoubtedly highly vulnerable, are typically teenagers who have actively engaged in risk-taking behaviour online and are deliberately arranging to meet with adult partners, knowing that sexual activity would be part of the purpose of the meeting. From this they conclude that the commonly projected picture of older adult men 'grooming'³³ prepubescent girls, or forcibly and violently abducting them, or forcibly and violently abducting younger teenagers, is just too simplistic. The ISTTF report cites a study that states that in only 5%

of the cases where men were arrested after meeting a young victim online had the victim been 'deceived by offenders claiming to be teens or lying about their sexual intentions'.³⁴

Child Exploitation and Online Protection Centre annual report

In its annual report for 2007/8, CEOP records that in the UK it had arrested 297 child sex offenders, a threefold increase on the previous year. CEOP also received a total of 5,812 reports from a range of sources, and covering several different kinds of child protection issues.³⁵ This was a 76% increase on the previous year and most probably reflects an increased awareness of CEOP's existence and of its online reporting mechanism.³⁶ While the CEOP statistics offer clear evidence of abusive behaviour online, it does not offer an estimate of the scale of the problem because, as with other areas of abuse, there is likely to be significant underreporting. Self-reporting studies have shown that one in four children say they have met people offline whom they had previously only become acquainted with online.³⁷ While the great majority of these meetings appear to have passed off without any cause for concern, it is worrying that in very many cases the children did not inform an adult of what they were doing.

There is currently no full assessment of the prevalence and impact of the different online risks and harms to children in the UK.

The UKCCIS research programme should give priority to determining overall prevalence levels for different types of risks to children online and to determining the extent to which a range of factors render children and young people more or less vulnerable to such risks.

³² ISTTF report, pg 16

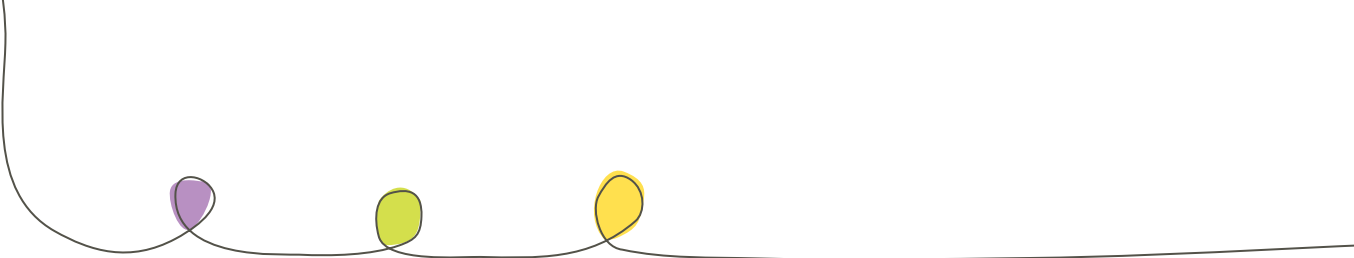
³³ No further breakdown of these figures is available.

³⁶ CEOP Strategic Overview 2007–2008.

³⁷ CEOP Strategic Overview 2006–2007, based on a sample of 6,000 children aged between 11 and 16.

³² ISTTF report, Appendix C, pg 18

³³ In the UK, the offence of grooming is defined in s.15, Sexual Offences Act 2005. It addresses situations where adults persuade children under the age of 16 to meet them for an illegal sexual purpose.



Law enforcement agencies should be required to record all instances where the internet or new technology played a significant role in sexual abuse or other crimes involving children. This information should be recorded centrally by the Home Office. The data should include information about the age and any other relevant characteristics of the victims and the perpetrators. It should also be published broken down by reference to the constabulary area where the crime was committed.

The social work professions, youth workers, health service personnel and others who engage with children and young people more generally need to become more closely engaged in the analysis of risks to children and young people on the internet and in the discussions about how best to provide some of the solutions. In particular, these groups need to be familiar with both the manifestations of online abuse in victims, and of the kinds of abuse engaged in by perpetrators.

Shared responsibility – and a combination of approaches

Regardless of the reasons why children and young people come to be exposed to risk in an online environment, and regardless of the ways in which different children experience or negotiate the risks, all players in this space must recognise their responsibility to do what they can to improve every child's safety.

For example, even if it were true that children and young people who are at risk online are the same as the ones who are at risk offline, this does not mean – as some have suggested – that high-tech companies therefore have no special or particular responsibility to address these issues simply because they may map onto broader societal problems.

Many would argue the technological dimension can only be effectively addressed by involving the firms that are the creators and providers of that technology. Those providing services on the internet that are targeted at or are used by children are creating social spaces for children, and consequently they must also take responsibility for the kind of environment they are promoting and the kinds of interactions they endorse or facilitate. CHIS believes that the technology companies are and must remain major players in providing technical safety solutions and in promoting a safe online environment.

Parents, schools and the education system more generally, together with law enforcement, children's and youth organisations, also have a major part to play. The voluntary sector in particular can have a key role in providing support and education to children and young people who may not be reached through mainstream services. The voluntary sector can be particularly adept in also engaging with children and young people themselves to develop, design, evaluate and deliver appropriate information and awareness materials.³⁸

In relation to the immediate care and supervision of children's use of the technology, parents, carers and adults working with children must inevitably remain centre stage. It is therefore essential that parents, carers and adults working with children are equipped to support children and young people when they go online, build their resilience and help them to navigate their way around the challenges it can present.

³⁸ Although industry has a key role in doing this too.

Education and awareness

The question of the effectiveness of different approaches to education and awareness programmes, and how well they reach parents, carers, adults working with children and children themselves, therefore becomes critical. If, for example, all of a company's safety information aimed at parents is published only in English, and a child's parents do not speak or read English, then that neglects the needs of that child and that family. Equally, if a child has a learning difficulty or some other vulnerability, very general advice about online safety will not be sufficient, either for the child or the parents/carers of that child. There is a responsibility on the part of the internet industry in particular, but it extends to all the relevant stakeholders, to accept their responsibility to initiate and sustain effective education programmes that are appropriate to the individual needs of every child and family using their services.

Futhermore, it is important that if education and awareness initiatives continue to be promoted as part of an overall solution, everyone can be confident that programmes are available that are appropriate in their approach and scope. This means they must be robustly and independently evaluated in order to determine their effectiveness.

In order to inform future design and implementation, it is important that there is a full and independent research-based evaluation of current education and awareness programmes to determine what approaches are most effective.

Technical measures

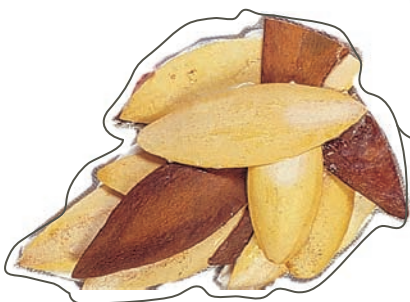
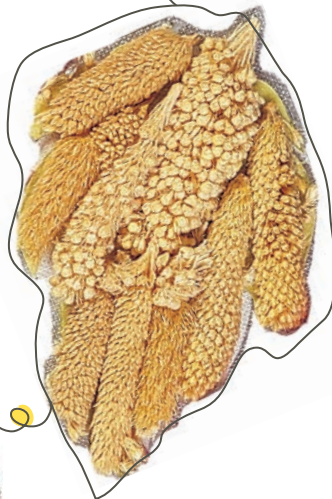
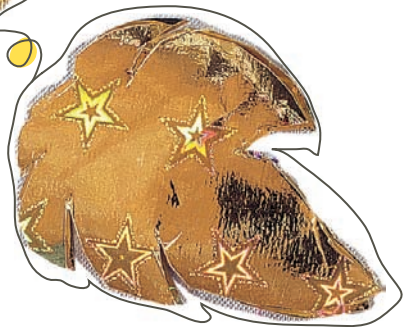
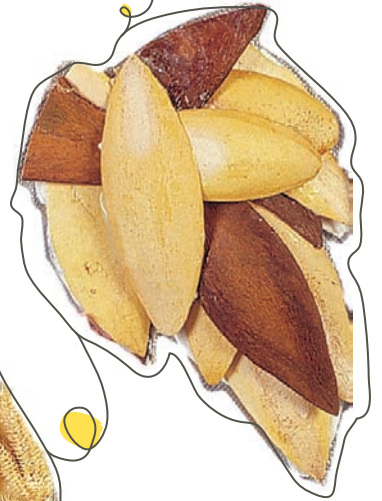
It is also important to supplement education and awareness initiatives with technical measures, such as filtering software, that are deployed to reinforce or underpin the core messages of internet safety education and awareness work. Often education and awareness programmes are mooted as the superior alternative to the deployment of technical measures such as filtering. This is far too simplistic. There is a valid and vital place for both. In this respect, CHIS endorses one of the key conclusions of the ISTTF – while they were speaking specifically about social networking sites and with a particular focus on age verification solutions, their words will ring true across online services as a whole when they state:

‘...there is no one technological solution or specific combination of technological solutions to the problem of online safety for minors. Instead, a combination of technologies, in concert with parental oversight, education, social services, law enforcement, and sound policies [by online service providers] may assist in addressing specific problems that minors face online. That formula gives no one an easy way out. Everybody has to do their best under each of the headings.’³⁹

³⁹ ISTTF report, pg 6



Section 3



as long as it takes

Section 3

Government and stakeholder responses

The UK's self-regulatory codes of practice

The Home Secretary's Task Force on Child Protection on the Internet was established in 2001 as the key government agency charged with driving forward the UK's self-regulatory approach to policy development in this area.

The Task Force brought together the key players in the internet space: leaders from the ISP and software communities, from the police and central government, academics and child advocacy groups. In 2003, the UK's mobile phone networks also joined, as they too had become major providers of internet services. From the outset, the Task Force contained direct representation from the Conservative and Liberal Democratic parties in Parliament, emphasising the importance many people attach to keeping this area of policy out of the party political arena.

Prompted by the major media coverage surrounding some of the early cases of children being sexually abused by adults whom they had met for the first time on the internet, the Task Force was quick to fund⁴⁰ several public information campaigns that addressed that type of threat.

However, the bulk of the work of the Task Force was driven by a series of sub-groups that looked in great detail at children and young people's interactions with the internet, across a very broad spectrum of issues. These sub-groups produced codes of good practice that were intended to guide existing and new technology companies in how they

might deliver their services. Over the years, a number of codes emerged from the groups. The topics covered included:

- ▶ web-based services
- ▶ the moderation of chat-based services
- ▶ the ethical use of case studies involving children
- ▶ adult content and services provided over mobile phone networks
- ▶ managing child-focused location services provided via mobile phone networks
- ▶ how search engines should minimise access to child sex abuse images
- ▶ the operation of social networking sites

In addition, through the Task Force the Home Office and Office of Communications (OFCOM) sponsored a working group that, together with the British Standards Institute, devised a kitemark for filtering software.⁴¹

The strength of these codes was that, because they were developed by consensus between the industry, police, government and children's organisations, they enjoyed a broad level of support and backing. However, one of the major shortcomings was that there was never any mechanism agreed upon that would systematically monitor or assess the impact of implementing the codes. As a result, with the exception of the code on content on mobile phones, where OFCOM initiated a review, it was impossible to tell whether or not, or to what extent, any of the other codes were being implemented, even by those who had taken part in their formulation.

The Byron Review rightly pinpointed this as a major weakness in the UK's self-regulatory arrangements. It was as much down to a lack of resources being invested in the system by the Home Office as it was to do with the industry's willingness to submit to the rigours

⁴⁰ Always through under-spends obtained from other Home Office budgets – the Task Force never had its own dedicated staff or its own dedicated resources.

⁴¹ See www.bsi-global.com/en/ProductServices/Kitemark-for-Child-Safety-Online



of independent assessment, but both factors were most certainly in play. Moreover, in addition to not knowing whether or not the codes were being honoured, equally there was no evidence as to whether or not the codes were having any impact at all. Despite a general belief that they did have an impact, there was no reliable way of testing this.

CEOP

A major new institution that emerged from work within the Task Force, and more specifically from campaigning by CHIS, was CEOP. Key elements of the internet industry also very strongly supported the establishment of CEOP. As a law enforcement agency, a major focus of CEOP is on confronting online grooming. CEOP also has a dedicated unit for identifying children from child abuse images and undertakes operational work on investigations involving child abuse images.

Responsibility for dealing with online bullying is spread across a number of agencies and CEOP would only become involved if the behaviour complained of were of a particularly serious nature. Undoubtedly CEOP is a success story – and a world first. However, there are still concerns about CEOP relating to its as yet unresolved longer term resource needs.

CEOP's core funding should be sufficient to cover all of their operational needs and should not leave them dependent on external agencies to resource any significant areas of their work.

Local police forces

The overall success of the policing effort to combat child abuse online depends heavily on close and productive working relationships between CEOP and each of England's police forces, and the police forces in Scotland, Wales and Northern Ireland. It would greatly

assist police work in this area, and it would greatly assist the cause of child protection more generally, if child protection were included as a statutory performance indicator for all Chief Constables.

The Home Secretary should make child protection a statutory performance indicator that is reflected in the priorities of every local police force in England and Wales and an equivalent measure ought to be adopted in Scotland and Northern Ireland.

When the police conduct an operation involving online criminal behaviour, almost invariably they will seize computers and storage media that then need to be analysed. In child protection cases, in the interests of any victims and indeed in the interests of the alleged perpetrators,⁴² it is extremely important that this analysis is conducted as speedily as possible to retrieve any time-sensitive data, including data that might disclose information about previously unknown victims or offences. The volumes of data involved can be staggeringly large, requiring perhaps hundreds, even thousands, of police hours simply to view the pictures and videos that might form only part of the content. In addition, there is a need for detailed forensic analysis. There are signs that the available forensic capabilities of local police forces are buckling under the strain, leading to longer and longer waiting periods.

Additional resources are urgently required to enable the police or other investigating authorities to improve the speed with which they can conduct forensic and other examinations of digital devices that are part of a criminal investigation into child abuse.

⁴² Waiting to be charged or waiting to go to trial for child abuse charges can be very stressful for the accused. Such individuals will now, routinely, receive counselling and, if held in custody, they will be put on 'suicide watch'.

The Byron Report

In September 2007, the Prime Minister, Gordon Brown, appointed child psychologist Professor Tanya Byron to do the following:

- ▶ to undertake a review of the evidence on risks to children’s safety and wellbeing of exposure to potentially harmful or inappropriate material on the internet and in video games
- ▶ to assess the effectiveness and adequacy of existing measures to help prevent children from being exposed to such material and help parents understand and manage the risks of access to inappropriate content, and to make recommendations for improvement or additional action

Professor Byron published her report in March 2008.⁴³ Because of the terms of reference of her review, it was not possible for Professor Byron to cover every area of concern regarding online risks to children.⁴⁴ However, her report was perhaps the first one in the world to link, in a closely argued, evidence-based and scientific way, what we know about child development, particularly the development of children’s brains, and the specific environments the new technologies are creating.

All of Byron’s recommendations were accepted and endorsed by the Government, and the Byron Review has received widespread support from all the major political parties.

⁴³ *Safer Children in a Digital World* (The Byron Review), DCSF, March 2008

⁴⁴ Many of the concerns Professor Byron was unable to cover are addressed in Sections 4 and 5 of this manifesto.

The detailed recommendations in the Byron Report will not be repeated in full here, however she set out three overarching objectives:

- ▶ **Objective 1 – Reduce availability:**
Reduce the availability of harmful and inappropriate material, the prevalence of harmful and inappropriate contact, and the conduciveness of platforms to harmful and inappropriate conduct.
- ▶ **Objective 2 – Restrict access:**
Equip children and their parents to effectively manage access to harmful and inappropriate content, avoid incidences of harmful and inappropriate contact, and reduce harmful and inappropriate conduct.
- ▶ **Objective 3 – Increase resilience:**
Equip children to deal with exposure to harmful and inappropriate content and contact, and equip parents to help children deal with these things and parent effectively around incidences of harmful and inappropriate conduct by their children.⁴⁵

CHIS strongly supports this approach. The report goes into a great deal of detail about the importance of engaging teachers and the education system as a whole in promoting both awareness of the safety agenda and the skills to deal with it. The report links this work to the wider safeguarding agenda and underlines the importance of finding effective ways of reaching out to parents and carers in order to help them protect their children. With this in mind, Byron recommends a major public awareness campaign on e-safety and the development of an authoritative ‘one-stop shop’ to signpost parents and children to information they need to keep themselves safe.

⁴⁵ Op cit, The Byron Review, para 3.99

In addition, the Byron Report speaks extensively about a wide range of issues connected to video games and online gaming.⁴⁶ Professor Byron made a great many, often quite specific, recommendations in respect of the advertising, promotion and use of video and online games. Byron also recommends changes in the way games are classified, including calling for greater efforts on the part of the retailing and games industries to improve the way information about games is presented to parents and children alike. In particular, Byron recommends ‘focused efforts to monitor enforcement of the statutory age ratings at the point of sale’.⁴⁷

The role of age verification in helping to make social networking sites safer for children⁴⁸ was considered and commended by Byron as potentially having an important role to play, but it was suggested that, at that time, there was no easy or obvious route to make it work on a very large scale. Companies were recommended to keep age-verification technology under review and, if appropriate to their site, to move to adopt it as the technology developed and improved. The potential of age verification to act as a means of obtaining compliance with laws concerning the supply over the internet of a range of age-restricted goods and services was not considered in any detail in the report.

Many of Byron’s insights and recommendations will become key reference points for future debates and developments in this space. One major principle that underlines her review is to acknowledge that not all harms in this area are

easy to measure and prove, but this cannot be accepted as an excuse not to act. We have to consider the probability of harm and make our policies accordingly.

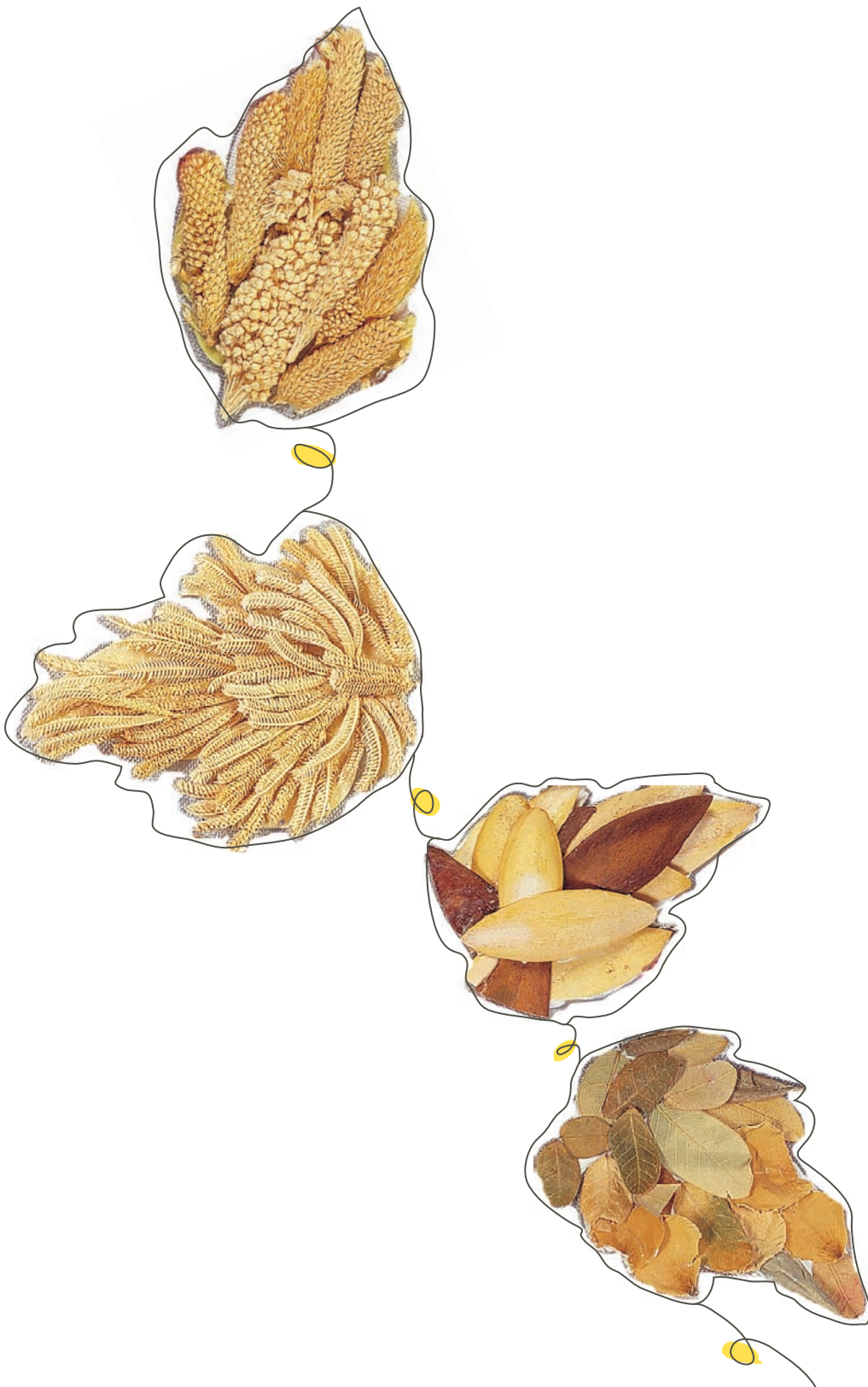
One of the institutional changes that Byron recommended was the winding up of the Home Office Task Force and the creation of a new body that would be jointly chaired by the Home Office and the Department for Children, Schools and Families. This new body, called the UK Council for Child Internet Safety (UKCCIS), was launched on 29 September 2008. It will report annually to the Prime Minister, giving it a new and very welcome high political profile. A new cross-departmental secretariat supporting the Council was suggested and is now in place. This will doubtless help counteract some of the problems with the old Home Office Task Force, which had no dedicated resources at all. The Government also decided to establish a UKCCIS Executive Board to help devise a strategy for and oversee the implementation of the report’s recommendations. The overall level of resources that will be devoted to UKCCIS is still unclear but, obviously, this will be of critical importance to the success of these new structures.

As already described, one of Byron’s main conclusions was that the old Task Force method of agreeing codes of practice without also agreeing on mechanisms for determining whether or not the codes were being implemented or having any effect, was no longer an acceptable option. She recommends a move towards independently monitored codes of practice and CHIS strongly endorses this approach. However, while the review called for an independent assessment of the codes, there are other places in her report where Byron retreats from such an interventionist position and the reasons for doing so are not always convincing.

⁴⁶ Ibid, Chapters 6–8

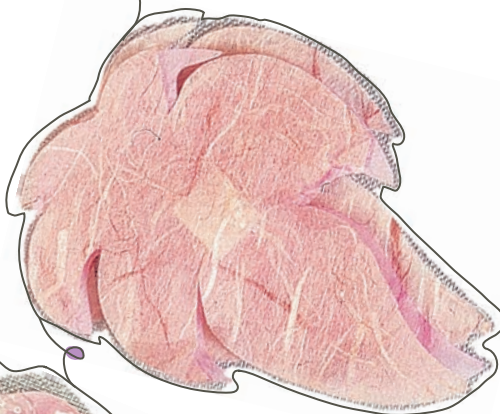
⁴⁷ Ibid, Executive summary, para 36

⁴⁸ The issue that was the genesis of the ISTTF report in the USA and had been the subject of protracted, sometimes very heated, debates between the US Attorneys General and the big US social networking sites.





Section 4



as long as it takes

Section 4

Child abuse images

Progress in the UK

The internet has completely transformed the scale and nature of the production and distribution of child abuse images. In 1997, in *People Like Us*, Sir William Utting described ‘child pornography’ as being a ‘cottage industry’.⁴⁹ That was probably the last moment in history when such a claim could be made. Today it is global. In the 2005 digital manifesto, child abuse images were highlighted as a major problem that mapped directly to the growth of the internet. The level of offending has continued at a worryingly high level.⁵⁰

Everything to do with the possession or distribution of child abuse images is unlawful, both in the UK and in very many other countries around the world. It is therefore clearly very difficult to determine the size or shape of what is essentially a clandestine and illegal business. All kinds of estimates have been made at different points about of the number of websites involved,⁵¹ and the total monetary value of the market in the images. No one familiar with the terrain doubts that the ‘business’ is worth many millions of dollars, certainly sufficient to attract the interest of organised crime.⁵²

Equally, there can be no doubt at all that the number of illegal images now in circulation on the internet runs into the millions and the number individual children depicted in those images runs into the tens of thousands.⁵³

⁴⁹ HMSO, 1997

⁵⁰ See above pg 16–17

⁵¹ In its annual report for 2007, the IWF maintained that fewer than 3,000 English-language websites accounted for the bulk of child abuse images available online. Three years earlier, the Computer Crime Research Center said the number was greater than 100,000.

⁵² See details of the ‘Reg Pay’ case: www.usdoj.gov/criminal/ceos/Press%20Releases/ICE%20Regpay%20PR_080906.pdf

⁵³ In correspondence with Interpol it was disclosed that their database contained over 500,000 unique child abuse images. Telefono Arcobaleno, in their report, speak of 36,000 children of whom ‘42% are under 7 years of age and 77% are under the age of 12’ (see www.telefonoarcobaleno.org/pdf/tredicmoreport_ta.pdf). Clearly the real numbers of both images and children involved are likely to be higher. These figures relate solely to what is currently known by the authorities from images already seized and processed.

Originally, the main way of distributing child abuse images over the internet was from within usenet newsgroups. The IWF was established in the UK in 1996 specifically to deal with this phenomenon by issuing notices to ISPs whose servers were unwittingly being used to facilitate the exchange. On receipt of such a notice, providing the ISP acted promptly to take down the identified image, they would escape any civil or criminal liability. At the time the IWF was founded, a little over 18% of all child abuse images found in the UK were being published out of the UK. Today, the proportion hovers below 1%.⁵⁴

Although the traffic in illegal images in and out of usenet newsgroups was significant, it was fairly contained. The arrival of the world wide web in the early to mid 1990s changed everything. Suddenly the internet was easy to use. This, more than anything, propelled the internet into the mass consumer market. Criminals engaged in the production and distribution of child abuse images, anxious to capitalise on the easier access the web provided, quickly made the web a major focus of their sales and promotional activities.

The IWF continued to operate its ‘notice and take down’ service in respect of individual images within newsgroups and it had also found a way to block access to whole groups that regularly contained child abuse images or advertised the availability of such images. However, ‘notice and take down’ was never going to be an effective weapon against child abuse websites because almost all of them were based overseas where, clearly, the IWF’s writ would not apply.⁵⁵ Yet the images on these websites were still available to UK residents, and the new challenge for the IWF was to see if there was a way to block access to these websites.

⁵⁴ IWF annual report 2008, published April 2009, www.iwf.org.uk/media/news.258.htm

⁵⁵ Other countries have equivalent bodies to the IWF but the speed at which they are able to act to get material removed has rarely matched that of the IWF.

The web, Cleanfeed and the IWF list

In 2004, BT showed how it could be done when they pioneered a system that they called 'Cleanfeed'. Essentially, BT took the IWF's list of known child abuse websites and configured their internal systems to block access to those addresses. BT never claimed that Cleanfeed was a perfect solution. Someone with sufficient determination and the right technical knowledge could find ways around it, for example by using other technologies.⁵⁶ The fact that the number of arrests remains as high as it does shows that these other routes are being used, but this in turn also underlines the importance of continuing to make the web itself a hostile environment to those intent on using it to exhibit, share and sell child abuse images.

On 11 May 2006, Home Office Minister Vernon Coaker indicated that on or by 31 December 2007, he would expect all UK-based ISPs to have developed a procedure for integrating the IWF list of already identified child sex abuse websites into their services in such a way as to block accidental⁵⁷ or casual access to them by their subscribers. As at 3 February 2009,⁵⁸ only 95% of consumer-facing ISPs had managed to do this and parts of the business-to-business ISP community were refusing to accept that the same policy ought to be applied to them. Ninety-five per cent sounds like an impressive figure, and indeed in many ways it is. Few countries in the democratic world can match it,⁵⁹ and both the

UK Government and the industry deserve a great deal of credit for that. However, the 5% gap means that around 700,000 households in the UK are potentially operating systems that allow access to known child sex abuse websites. This is simply too many. Moreover, that number and the calculation are based solely on the number of households with a broadband connection – in fact there are still a further three million households in the UK that do not connect to the internet via broadband so the real number of households that could connect to these sites is likely to be higher.

Given that so many ISPs are already deploying the IWF list, there is clearly no reasonable technical argument against implementing such a policy. Some smaller ISPs seemingly claim that cost is a major factor for them – this situation is unacceptable as it suggests that dealing with child sex abuse images is an optional extra. These costs should be seen as part of the basic costs of doing business.⁶⁰

The Government should prepare a Bill that will compel all internet service providers based in the UK to adopt the Internet Watch Foundation list, or some other technical solution that blocks access to all known child abuse websites and newsgroups. The Bill should also detail or make provisions for a method by which compliance with this policy can be tested and publicly confirmed. If it becomes clear that some ISPs will refuse to implement a blocking solution unless compelled by law to do so, the

⁵⁶ File-sharing software now plays an important part in the supply chain. This is much more difficult to deal with at a technical level, although work is going on to find an effective solution.

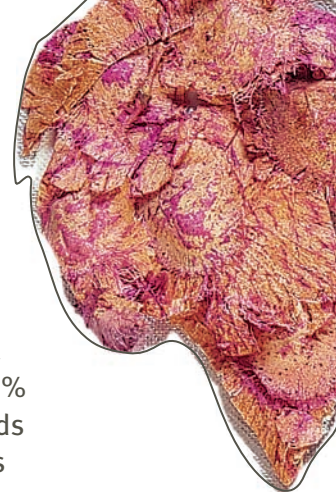
⁵⁷ It will also block the great majority of deliberate attempts to access such sites but the term 'accidental' is used essentially to suggest that if someone is sufficiently determined and has the right level of technical knowledge and skill, they could find a way around. Just how many people fall into that category is unknown.

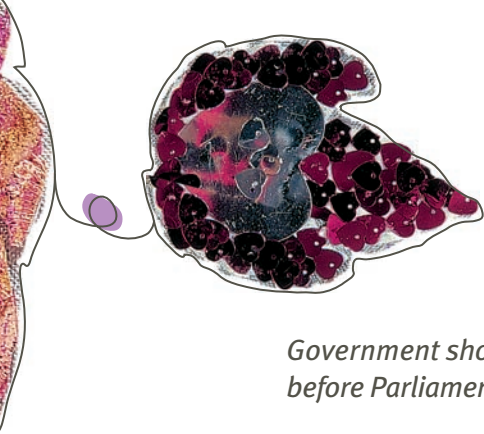
⁵⁸ Answer to Parliamentary Question from Margaret Moran MP.

⁵⁹ In Italy, since 2006 the blocking of child abuse web sites has been required by law and applies to all ISPs. In April 2009, the German Government indicated that they intend to follow Italy's lead. Elsewhere, on a voluntary basis,

Denmark appears to have achieved 98% coverage of its population and several of the Scandinavian countries also have high levels of voluntary compliance. In March 2009, the Commission of the European Union published a draft Framework Decision that could eventually see every member state required to make provisions to block access to known child abuse images websites. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0135:FIN:EN:PDF>

⁶⁰ However, given that cost might genuinely be an issue for smaller ISPs, perhaps the Government could devise some kind of tax incentive to encourage investment in the necessary technology. Alternatively, it could be added to or incorporated into the costs the Government is already covering in relation to the installation of extra kit to store records of data transactions pursuant to the EU Directive and RIPA, 2000.





Government should immediately put the Bill before Parliament.

In the meantime the Government should issue an instruction to all departments forbidding them from purchasing internet services from any ISP that does not deploy a solution that blocks access to all known child abuse websites. The Government should also encourage the remainder of the public sector to follow its lead.

The Government should consider the use of tax or other incentives to encourage ISPs and other technology companies to develop and deploy new or speedier ways of tracking, blocking or destroying online child abuse images.

Other internet environments

Within the UK and elsewhere, more and more of the trade in child abuse images is shifting to peer-to-peer environments and to closed groups of various kinds.⁶¹ These are inherently more difficult to police. It is important that future strategies effectively address the issues relating to peer-to-peer and closed groups.

The Government, law enforcement and the industry should begin discussions about how to combat the use of peer-to-peer software for the distribution of child abuse images and about how to combat the emergence of other types of closed groups or communities that have the same purpose. An immediate start could be made by looking to the industry to fund a specific, time-limited operation⁶² similar to that deployed by the music and film industries to protect their copyrighted material from unlawful exploitation by file-sharing software.

⁶¹ Sites that advertise pornographic images of young people as being 'barely legal' are often just a shop front that can quickly channel a visitor to other places on the internet that are wholly or largely concerned with supplying illegal material. For this reason, this type of branding of sites is particularly undesirable.

⁶² Time limited so that a review of its efficacy can be judged before deciding whether or how to continue with it.

The high-tech industries should urgently address ways to prevent the misuse of anonymity, encryption software and other technologies from facilitating the exchange of child abuse images.

Victim identification

Another concern for CHIS is the progress that still needs to be made to identify, locate and help to recover the victims of online child abuse images. Only a small number of children have been successfully identified from images held in the Interpol database, and the same is true for many of the databases held at national level.⁶³ When the police seize a single computer, it can contain upwards of a million individual images and hundreds of hours of video. Looking at such volumes of still pictures, and above all the videos, is highly time consuming but its importance can hardly be overstated. Buried within the images and the videos may be information about children whose abuse has not yet come to the attention of the police or authorities, or new evidence about cases that are already known.

Various police agencies, including Interpol, now have substantial databases of illegal images. They are able to produce what are known as 'hash values' for each individual image. A hash value is a unique digital fingerprint, allowing rapid comparisons to be made between newly acquired collections of images and the existing stock of known images. Not only does this save valuable police time by helping them to avoid re-investigating images that might have already been investigated in another part of the world,

⁶³ The US-based National Center for Missing and Exploited Children said, in September 2008, that they knew of 1,660 children who had been identified from child abuse images, not all of which had been distributed on the internet (see 'Child Pornography and Sexual Exploitation of Children Online', paper for 3rd World Congress, www.ecpat.net). From correspondence with the authors, Interpol estimate they have identified around 900 children from the images that have come to them.



or indeed have been investigated by another police force within their own country, it also helps to identify new images that have not previously been investigated. Any new image carries with it the possibility that it has been produced recently and that therefore there are children currently being abused who, if they can be identified and located, might be rapidly rescued from the abuse. However, what these databases of digital images could also do is allow for the possibility of proactively searching the internet for replicas. This type of activity should be endorsed and encouraged by Government and law enforcement.

Drawing on the technical research currently being funded by the EU's Safer Internet Programme and others, the Government should provide more resources to help develop ways for law enforcement to achieve a higher rate of detection and location in real life of children who have appeared in child abuse images on the internet.

It is also the case that professional knowledge of the specific support and therapeutic needs of children abused in images is limited and the research available is not well disseminated. In the UK, due to a shortfall in therapeutic resources, it appears that children who have been abused in images are unlikely to be receiving an appropriate therapeutic intervention to help them recover from their abuse.

The Government should fund more research into the long-term consequences for, and therapeutic needs of, children who have been sexually abused where images of that abuse have appeared on the internet. The Government should also ensure that appropriate resources are developed to address these needs and that the children's workforce is trained to identify such therapeutic needs and knows how and where to refer children in order to ensure they receive appropriate forms of support.

The link to risks to children and young people

Within the UK, following advice from the Sentencing Advisory Panel that was adopted by the Court of Appeal,⁶⁴ all child abuse images are allocated to one of five levels. These reflect the seriousness of the abuse depicted in the image. The worst kind of images, at Level 5, will involve sadism or bestiality, Level 4 will portray a child engaged in penetrative sexual activity and so on to Level 1, where the images will depict erotic posing with no visible sexual activity. Repeated reports from lawyers appearing in cases involving this type of material, and from police officers, suggest that, when it comes to sentencing and assessing supervision requirements, judges, but perhaps particularly the probation and prison services, take the image as a key indicator of future risk. Some child protection experts, however, argue that, in fact (at least in terms of assessing future risk to children) the opposite might be true.⁶⁵ If a person is likely to act out the fantasies fed by their use of the images, Level 5 type activity would be much harder to organise than lower order forms of abuse. It would also be much more difficult for a perpetrator to rationalise, minimise or deny the impact on children of such extreme forms of behaviour.

Downloading images is a horrific offence against the children depicted and it deserves police attention entirely in its own right, but there is also evidence that suggests that people who get involved in downloading such images may find themselves on a path that ultimately leads them to commit offences against children either in the real world or online. Various studies have been carried out that explore the link between the possession of child abuse images and contact offending. The studies have come out with significantly different results but with some of them either



⁶⁴ In *R vs Oliver, Hartrey and Baldwin*, [2003] 2 Cr App R(S) 15

⁶⁵ Findlater, *Stop It Now – NOTA Conference*, 2007, also confirmed in correspondence with authors.

the methodology is problematic or they have been carried out on a very small scale, and many of them have been carried out in North America, where the laws and approaches to sentencing can sometimes be very different.⁶⁶ However, work carried out in the UK by Professor David Middleton also suggests that with UK-based perpetrators there are similarities between the psychological profiles of convicted child sex offenders and those convicted of offences relating to child abuse images.⁶⁷

Large-scale research is needed to determine whether or to what extent there is a link between the offence of possessing child abuse images and committing other types of sexual offences against children. Research should also seek to establish if the possession of different types of child abuse images can be used as a predictor of likely future risk to children.

International work to tackle child abuse images

ICANN's role

In its annual report for 2008, the IWF noted that child abuse images were being made available commercially on websites from within a comparatively small number of domains: '75%... (some 850 unique domains) are registered with just 10 domain name registries'.⁶⁸

⁶⁶ See for example, *Self-Reported Contact Sexual Offenses by Participants in the Federal Bureau of Prisons' Sex Offender Treatment Program: Implications for Internet Sex Offenders*, Hernandez, November 2000, presented at the Association for the Treatment of Sexual Abusers (ATSA) in San Diego, California; *From Fantasy to Reality: The Link Between Viewing Child Pornography and Molesting Children*, Kim, C (2004), based on data from the US Postal Inspection Service; and *Internet traders of child pornography and other censorship offenders in New Zealand: Updated Statistics* (November 2004), Wilson and Andrews.

⁶⁷ Middleton, D, Elliott, IA, Mandeville-Norden, R and Beech, AR (2006) 'An Investigation into the Applicability of the Ward and Siegert Pathways Model of Child Sexual Abuse with Internet Offenders Psychology', *Crime & Law* Dec 2006.

⁶⁸ www.iwf.org.uk/media/news.258.htm

This speaks of a regulatory failure by the Internet Corporation for Assigned Names and Numbers (ICANN),⁶⁹ the global body responsible for the operation of the naming system on which the internet depends. The EU, national governments and others should make representations to ICANN to deal more effectively with this issue.

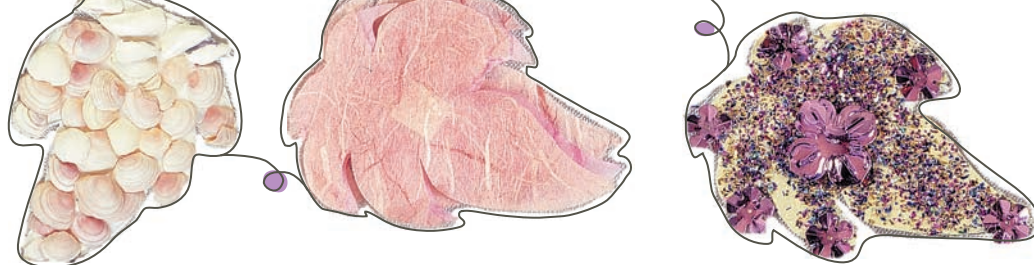
Technical measures

The EU's Safer Internet Programme has become a major source of funding for the development of new technologies that will assist law enforcement both to process the huge amounts of materials that are often seized in police operations across the world, and to ensure that the intelligence gleaned from it is routed to the appropriate police agencies as swiftly as possible.

The I-Dash project will develop a set of automatic tools to support police professionals in their investigations involving large quantities of child sexual abuse material contained in videos. The MAPAP project will help analyse illegal content on peer2peer networks. The FIVES project will help with the sheer volume of illegal material obtained during forensic enquiries by identifying and distinguishing new material from already known material. The Commission will also co-fund the establishment and maintenance of an International Child Sexual Exploitation Image Database, managed by Interpol. This will be an upgrade of and greatly enhance the existing database, which receives input from police forces worldwide. The Commission is also funding a project called CIRCAMP that, under the auspices of Europol and Interpol, was established to encourage organised, extensive cross-border exchange of best practice in the fight against the production

⁶⁹ www.icann.org





and online distribution of child sexual abuse material within Europe and internationally. Currently CIRCAMP brings together police forces from 11 countries. Already they have the capability to interrogate in real time a shared database of known images, and at the time of writing six countries had already developed the capability to use it.⁷⁰

G8 and the Virtual Global Taskforce

The G8 has also sponsored initiatives to support further research into online child abuse. One of the key offshoots of the G8's engagement with online child protection was the emergence and development of the Virtual Global Taskforce.⁷¹ It was championed by CEOP and currently, in addition to Interpol, it also has member agencies in the USA, Canada, Australia and Italy. The VGT works in the area of child abuse images but it has tended to emphasise tracking travelling sex offenders and policing or receiving reports from real-time environments where children may be a risk from sexual predators.

Microsoft has also made an important contribution to this area of work through the development of its Child Exploitation Tracking Services (CETS), which it describes as being:

'...a database tool that enables agencies to avoid duplicate effort. Sharing information over a secure network, officers can match up investigations that reference the same people or online identities. Using CETS, police agencies can manage and analyze huge volumes of information in powerful new ways, such as cross-referencing obscure data relationships and using social-network analysis to identify communities of offenders.'⁷²

⁷⁰ For the full text of the EU's Safer Internet work programme, see http://ec.europa.eu/information_society/activities/sip/docs/call_2009/wp_09.pdf

⁷¹ See www.virtualglobaltaskforce.com/what_we_do.asp

⁷² www.csreurope.org/solutions.php?action=show_solution&solution_id=291

There is no doubt that the momentum behind international police co-operation in the field of child protection is building up, and it is not before time. There certainly have been spectacular examples of successful co-operation across borders by national and local law enforcement agencies that have led to the break up of large networks and to large numbers of arrests of persons involved in downloading child abuse images. Yet the number of children being identified and rescued and the number of arrests of the people behind the large-scale commercial production and distribution of child abuse images remain disappointingly low.

Law enforcement agencies are loathe to discuss openly why this is the case but there is a persistent feeling that, at least in part, it is because so much police activity in this area, in particular in respect of the allocation of police resources, remains constrained or confined by national jurisdictions. We have yet to see the emergence of an adequately resourced international police agency that has its own investigative capability that can target the multinational trade in child abuse images and which would also win and retain the necessary support of the various national police agencies.

Slow takedown times

Progress in obtaining the take down of identified illegal images has also been very patchy. In June 2008, academics from Cambridge University published the results of their research⁷³ into the amount of time it took for different forms of illegal content on the internet to be taken down once notified to the relevant authorities. The best performance was achieved by the banks acting on reports of phishing (identity theft) websites, where the mean lifetime of over 300 identified websites was between 3.5 and 4.3 hours. Seemingly one of the ways these impressive

⁷³ *The Impact of Incentives on Notice and Take-down*, Moore and Clayton, www.cl.cam.ac.uk/~rnc1/takedown.pdf

speeds were achieved was through the simple expedient of using the telephone to ring up the online service providers identified as unwittingly providing hosting services.

Almost the worst performing section was child sex abuse images, where the mean lifetime of over 2,500 identified websites was 719 hours. In some instances, child sex abuse websites that had been notified to the authorities were still up on the web 12 months later. This is completely unacceptable, although it is acknowledged that the reasons for this lie outside the direct control of the UK government and UK law enforcement.

Reinforcing the Cambridge University study, in March 2009 a German NGO called Care Child published the results of a collaboration with the Danish police, who handed them a small random sample of 20 overseas sites, taken from their main list of 3,500 known sites. Rather like the banks grappling with phishing sites, the German NGO simply contacted the website hosts directly, bypassing the traditional routes. Seventeen website hosts were in the USA and one each were in Holland, the UK and South Korea/Portugal (HTML coding in South Korea, images in Portugal). Sixteen of the 20 sites were closed down within 12 hours, eight of them within three hours. Three sites said that they had documentary evidence that the 'models' employed on the site were over 18 years of age, as required by US law. Fourteen days after the test, it was learned that some of the sites had moved location and were back in business, but almost half had not.


For as long as the images remain on view, the children depicted in them are, in an important sense, being re-victimised. New people might find them and perhaps get involved in downloading or collecting these images for the first time. Getting the images removed or blocking access to the sites containing them, whichever can be achieved sooner, has to be a major priority.

It is understood that nothing should be done that might jeopardise a potential prosecution of an offender. On the other hand, neither should pictures of children being sexually abused be left on view for extended periods only because the local police are too busy with other work. Most emphatically, pictures of children being sexually abused should never be deliberately published or left on view simply to act as bait to catch new offenders. The current delays in getting material taken down are overwhelmingly linked to police workloads and they very rarely have anything at all to do with any ongoing police investigation.

The IWF should consider adopting new or additional methods to speed up take down times for child abuse images hosted overseas.

While the Cambridge report clearly suggests there is room for improvement, the UK otherwise has an exemplary record in getting child sex abuse websites or other content speedily taken down once discovered on any UK-based hosting service. The IWF can do this in part because it is the recognised body for first deciding whether or not a given image is illegal, then for notifying ISPs about the image or the URL, and dealing with them is practically the IWF's exclusive focus. By contrast, in many other countries in the world where hotlines⁷⁴ exist, the law seems to require that all reports of illegal content go first from the hotline to the police. The police then have the responsibility for deciding whether or not the image is illegal and, assuming it is, for notifying the relevant ISP or hosting company. This appears to be where the bottleneck and the delays occur. This is clearly not a criticism of any individual hotline within the EU or elsewhere, but it does raise concerns about how effectively different national law enforcement agencies relate to their national hotlines.

⁷⁴ The IWF is the UK's 'hotline'. According to the international association of hotlines, INHOPE, there are currently hotlines in 30 countries around the world.



As already noted, the IWF maintains a list of all known child abuse websites, irrespective of where in the world the material is hosted, and offers a copy of it to ISPs or web filtering companies that wish to deploy it as part of a planned policy of blocking access to such sites. It has also been noted how this list is widely deployed within the UK, but an increasing number of overseas ISPs and web filtering companies also use the IWF list. However, industry representatives in all parts of the world have repeatedly called for a single list that consolidates the lists of as many hotlines or police agencies as possible.

In order to promote the more efficient blocking of child abuse websites worldwide, the UK Government should engage with the EU and others with a view to expediting the creation of a single list of all known child abuse websites, or a list that is as large as possible, drawing on any and all national lists that are not encumbered by local legal constraints. With appropriate security surrounding its deployment, this resource should be made available to relevant online service providers, filtering companies and others with an appropriate interest in blocking access to or investigating websites containing child abuse images.

The Government should play an active role in promoting the greater harmonisation of national laws relating to, and police procedures for, dealing with online child abuse images. In addition, the UK Government should sponsor the development of an internationally-based investigative unit with a specific remit to focus on the criminal networks behind a very high proportion of the trade in commercially available child abuse images.

The Government should promote discussions at an international level with a view to improving substantially the speed with which, once notified to the relevant authorities overseas, child abuse images are removed altogether or access to them is denied.

The Government should promote discussions at an international level to find ways of preventing the trade in or hosting of child abuse images moving to countries with poorly developed laws on cyber crime or few resources locally to enforce such laws. In addition, the UK Government, the EU and others should make representations to ICANN with a view to securing a substantial improvement in the regulatory performance of those individual domain name registries that currently appear to be ineffective in preventing child abuse images from being published under their auspices.

Pre-paid cards

CHIS applauds the major efforts being made by the financial services industry, through the Financial Coalition Against Child Pornography and the work of the International Center for Missing and Exploited Children in the USA, together with its recently launched European counterpart,⁷⁵ to prevent the world's major online payments systems from being used to facilitate the trade in child abuse images. Nonetheless, the recent emergence of pre-paid credit cards, or stored value cards, which can be obtained anonymously for cash, appears to threaten to undermine some of that work.

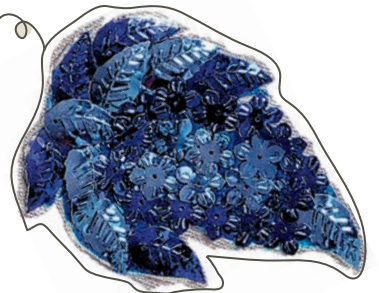
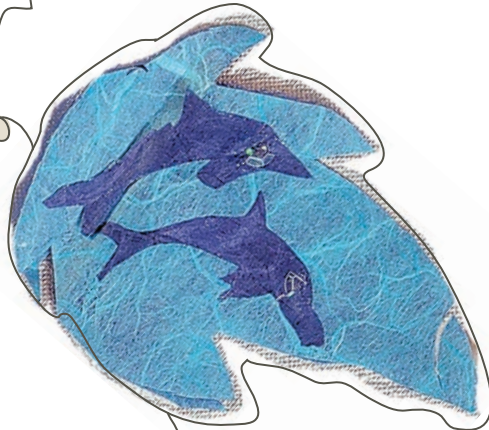
The Financial Services Authority should take a close look at the way pre-paid card systems, especially those that can be obtained and used anonymously, might be fuelling a growth in criminal exchanges on the internet, particularly around child abuse images.

⁷⁵ The European Financial Coalition, see www.ceopgov.uk/efc





Section 5



as long as it takes

Section 5

Part 1: New and emerging issues

Children's access to age-restricted goods and services

The speed with which e-commerce has taken off has been truly astonishing.⁷⁶ It constantly throws up fresh challenges that impact upon consumers of all ages. It has led to the formation of a new campaign for 'Digital Rights for Consumers' whose aims we support.⁷⁷

A new problem that CHIS has become aware of in recent years is the ability of children to use the internet to gain access to age-restricted goods and services that they would never be able to obtain on the high street because their appearance would betray their true age.

The law makes no distinction between offline and online environments, applying equally in both places. Companies or persons selling age-restricted goods or services are meant to create a system that allows them to exercise due diligence in terms of ensuring compliance with the age-restriction laws. Moreover, the system has to be capable of being tested and it must be shown to be effective. As recent evidence from the Trading Standards Institute⁷⁸ and others has shown, in the UK these laws are not being properly followed online.

In 2005, Parliament passed the Gambling Act. Included in its provisions were clauses that required all online gambling companies to carry out independent third party checks into the age of the persons seeking to place a bet using their site. Hitherto they had only been asking people to tick a box to confirm that they were 18 or above and therefore legally entitled to gamble. Many children were simply ticking the box and lying about their age. This came to light in part when parents started discovering that their children had

developed an addiction to gambling, spending their pocket money and other funds via their Solo or Visa Electron debit cards (which some banks routinely issue at age 11).

Legislation should be brought forward to provide for the development of regulations governing the online sale of age-restricted goods and services.

Data protection, privacy and consent in the online environment

Closely related to the concerns about children being able to access age-restricted goods and services online is the wider question of how companies or organisations of any kind obtain a wide variety of data from minors over the internet. This in turn touches on issues of privacy, data protection and how to obtain consent. The matters were discussed at length in October 2008 at the 30th International Conference of Data Protection and Privacy Commissioners, where a resolution proposed by the Privacy Commissioner of Canada was adopted that, among other things, called for:

'...educators to recognize privacy education as fundamental to a child's education and to include privacy education in their curricula;

...legislation... limiting the collection, use and disclosure of children's personal information, including appropriate provisions for violating those requirements;

...appropriate limitations on the collection, use and disclosure of personal information about children for the purposes of online micro-targeting or behavioural advertising;

...operators of websites created for children to demonstrate social responsibility by

⁷⁶ See above, pg 11 et seq

⁷⁷ For further information, email ed.mayo@consumerfocus.org.uk

⁷⁸ www.tradingstandards.gov.uk/policy/policy-pressitem.cfm/newsid/151

adopting privacy policies and usage agreements that are clear, simple and understandable, and educating users about existing privacy and security risks and website choices available to the users.’⁷⁹

Legal position

Providing the correct procedures and processes are observed, there is no necessary antithesis in UK law between anyone’s right to privacy or data confidentiality and the right of children and young people to be properly protected.

In the UK, children and young people engage in a wide range of ‘data transactions’ online but there is no clear-cut, legally enforceable minimum age that defines when verifiable parental consent must first be obtained. Everything hinges on the nature and complexity of the transaction and the capacity of the legal minor to understand it. Quite how a company or any other kind of organisation that operates online is meant to assess a legal minor’s capacity over the internet has never been satisfactorily explored or explained.

The ICO’s basic views on a number of these questions was set out in an issues paper published in November 2006 entitled ‘Protecting children’s personal information’⁸⁰ and a data protection good practice note published in May 2007 entitled ‘Collecting personal information using websites’.⁸¹

In the issues paper, the ICO points out that, within the UK, the data protection laws make no distinction between individuals (‘data subjects’) based on their age. In other words, in principle, adults and children have exactly the same rights. According to the

Commissioner, the law: ‘confers rights... [on the child and] ...these rights should only be exercised by another *on their behalf* if they are not capable of exercising them independently.’ However, the Commissioner also says that he ‘would always recommend as good practice that parents should be consulted about important decisions affecting their children’. Thus, for persons under the age of 18, strictly speaking the entity seeking the data is therefore supposed to satisfy themselves subjectively, child by child, that the individual child understands the nature of the transaction.⁸²

The age of 12

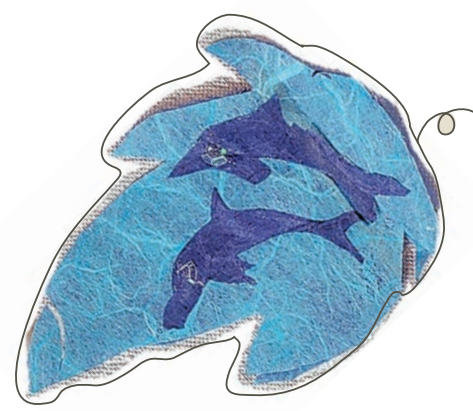
On a more practical note, the ICO maintains that, in general, 12 is the age at which a young person might reasonably be supposed to understand enough to be able to give consent on their own behalf, at least about a range of matters. In effect, this advice means that, at the moment in the UK, companies should always seek to obtain verifiable parental consent for any data transaction involving any child aged 11 or below. However, if the transaction is at all complex, for example if it might lead to a child’s data being transferred to a third party for whatever reason, verifiable parental consent ought to be obtained regardless of the age of the child. To amplify this point, in paragraph 8 of the good practice note, the Commissioner expressly says ‘If you need parental consent, you must have some way of verifying this. It will not usually be enough to ask children to confirm their parents have agreed by using a mouse click. If you need parental consent but decide that verifying the consent will involve disproportionate effort, you should not carry out the proposed activity.’

⁷⁹ See www.privcom.gc.ca/information/conf2008/res_cop_e.asp

⁸⁰ www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/issues_paper_protecting_chidrens_personal_information.pdf

⁸¹ See www.ico.gov.uk/upload/documents/library/data_protection/practical_application/collecting_personal_information_from_websites_v1.o.pdf, para 8

⁸² When it comes to buying goods and services, different or additional issues arise. Legal minors cannot enter into enforceable contracts, other than for (ill-defined) necessities, so very often they are obliged to obtain the co-operation and support of an adult if the transaction is to be completed. However, the reasons for that are connected to the law of contract and ought not to be confused with the data protection and privacy laws.



The ICO's advice about 12 year olds has been criticised by a distinguished panel of lawyers and children's rights advocates who point out that, while it has no basis in law, in effect it has become a de facto standard.⁸³ The suggestion is that, because of the ICO's stated view, all manner of organisations simply assume that a child of 12 or more is competent to give consent, make no further enquiries and miss the crucial element of assessment.

The advice in relation to the 12-years-of-age threshold predates the internet age. It was inherited from the old Data Protection Agency and quite how they arrived at it now seems to be lost in the mists of time. It looks increasingly out of step with the view being taken in other countries (eg Spain and the USA) where they have specifically considered the matter since the arrival of the internet.⁸⁴

Spain and the USA

The Spanish data protection authority, Agencia Espanola de Proteccion de Datos (AEPD), recently issued a handbook that gives detailed advice and guidance about the capacity of legal minors to give consent to online data transactions. It establishes that, in Spain, 14 is the legal minimum age at which a company or other organisation might ask a child directly for personal data pertaining to themselves. Below that age, it is first necessary to obtain verifiable parental consent and the handbook also provides advice on how such verification might be

⁸³ 'Protecting the virtual child. The law and children's consent to sharing personal data', Action on Rights for Children, January 2009, www.archrights.org.uk/issues/Virtual%20Child.htm

⁸⁴ However in September 2009, a new code of 'Good Practice Principles' will come into effect that will govern how behavioural advertising will work in the UK. For these purposes, the ICO appears to have endorsed the notion that 13 is the relevant minimum age. Admittedly, these are two different scenarios but it is perhaps an interesting indicator for the future. See www.iabuk.net/en/1/iableadsbehaviouraladvertisinggoodpractice030309.mxs

performed. In the USA, under the Children's Online Privacy Protection Act, 1998, the age limit is set at 13. These discussions about the age at which children are able to give consent in their own right has important implications for the safety of sites and forums aimed at children and young people.

The ICO should issue clear, research-based advice and guidance on the respective rights and responsibilities of all the parties where online data transactions involving legal minors are concerned. In particular, the ICO should consider setting, or asking Parliament to set, a legally defined minimum age below which verifiable parental consent will always be required in an online environment.

Electronic tracking – new location services

In the UK, we have had tracking services for several years specifically aimed at helping parents to keep their children safe. Some of these child-tracking services were, at least initially, marketed to parents in ways that misleadingly implied that knowing a child's approximate whereabouts⁸⁵ was the same as knowing that the child is safe.⁸⁶

⁸⁵ The accuracy of the location data could be highly variable depending on the configuration of the mobile phone network in a given area. In principle, however, in densely populated urban areas the data could be accurate to within 100 metres.

⁸⁶ All that a parent would know, in fact, is where their child's mobile phone handset is or, to be even more precise, they would only know where the SIM card from within the handset is. Either or both could be entirely divorced from the child or the handset in question having been, for example, stolen, lost or damaged.

Take up of these services has not been very widespread but nevertheless they continue to be provided. They work through the mobile phone networks and are one of a class of what are known as ‘passive’ location services.⁸⁷ These types of services are the subject of a code of practice that was agreed between the police, the Home Office and child protection agencies in 2004.⁸⁸ However, we are now seeing the emergence of new tracking technologies that do not depend on the co-operation or engagement of the mobile phone networks. Google has recently launched such a tracking service called Latitude, which works through mobile phone handsets, and Yahoo has a similar product called Fire Eagle. Because such services are based on one or more of GPS (satellite) tracking, open cell ID or wifi location, they are not covered by the code of practice. It may well already be the case that the mobile phone companies are no longer the main suppliers of location data.

The emergence of tracking technologies into the mass consumer market not only raises wider civil liberties issues but also, to the extent that they are available to children and young people, they also raise child safety concerns. In contrast to the original passive location services, which had to be paid for, typically with a credit card, the new breed of location services are financed through advertising so, for practical purposes, they are free to the end user and therefore, short of other measures being taken, they will be available to and used by children and young people.

⁸⁷ They are referred to as being ‘passive’ because, while the consent of the person being tracked is required at the outset, once that consent has been given, the third party can track the individual without any further direct reference to them – they will not know when or how often their movements have been checked.

⁸⁸ www.mobilebroadbandgroup.com/documents/UKCoP_location_servs_210706v_pub_clean.pdf

The emergence of these new services into the market has not been accompanied by rigorous consultation with child protection agencies, at least not in the UK, as was the case with the original code developed jointly with the mobile phone networks. Instead the existence of these new services came to the attention of CHIS member organisations only when they were contacted by concerned parents or by hearing about it through the media.

In 2006, Judy Mallaber MP introduced a Private Member’s Bill⁸⁹ to the House of Commons that, had it been passed, would have required a licensing regime to be established for all tracking services providing information about the physical whereabouts of children, irrespective of the particular technology being used.

The ICO has been strangely silent on this issue.⁹⁰ Unless a self-regulatory approach to addressing these issues can emerge rather quickly, there is a strong case for bringing this Bill back to Parliament.

Maintaining strong personal security online, being careful with what you post about yourself and being media literate are all messages that are fundamental to the safety agenda that is constantly promoted to children and young people. In this respect, the privacy of real-time information about a child or young person’s physical whereabouts should be a key concern commanding extra layers of security that at the moment do not seem to be in place.

⁸⁹ www.publications.parliament.uk/pa/cm200506/cmbills/144/06144.i-i.html

⁹⁰ We argue, while it certainly is a data protection issue, it is also much more than that. Either way the ICO needs to engage.





The Government should initiate an inquiry into the new location technologies now emerging into the mass consumer market that, typically, centre on or use mobile phone handsets. The inquiry should recommend what steps need to be taken both to ensure that such services are marketed responsibly and to ensure that adequate security safeguards are in place to protect children and young people.

The mobile internet

While recognising its potential advantages, CHIS is also increasingly concerned by some of the challenges presented by the emergence of the mobile internet. It is clear that in the UK and elsewhere, more and more consumers will be offered access to the internet via mobile devices, typically smartphones. This inevitably introduces an additional layer of difficulty or complexity when it comes to supporting or supervising children and young people's use of these devices.

The UK's mobile phone companies have largely acknowledged this additional layer of difficulty or complexity. A majority of mobile operators have set by default an adult bar governing all content that they supply themselves through their own networks. Several also provide an adult bar that governs sites that can be reached on the internet.^{91, 92}

⁹¹ CHIS believes it would be good practice to set, by default, an adult bar to govern both kinds of services, and urges the mobile operators to ensure they are doing this. In the OFCOM review of codes of practice, it discusses progress on page 7 of the review *Default content controls put in place by operators*: 'All mobile operators have mobile commercial content controls set to default "on" at the time of purchase for pay-as-you-go customers. All but one have the same policy for contract customers. In relation to mobile internet content filtering, all operators except one have this default "on" at the time of purchase for pay-as-you-go, and two operators have content controls set as "off" for contract customers.' See www.ofcom.org.uk/advice/media_literacy/medlitpub/ukcode/

⁹² See CHIS submission to the Mobile Broadband Group for further details: www.nspcc.org.uk/Inform/policyandpublicaffairs/Consultations/2008/CHISInternetSafety_wdf61909.pdf

However, as more phones are produced and sold that have a wifi capability built in,⁹³ it will be increasingly easy for end users to bypass the safety settings that apply to internet access by simply logging on to any available wifi network. While many of these available wifi networks will themselves have general security settings linked to them, it is very unlikely their settings will match those of the mobile operators.

CHIS rejects the notion that a mobile phone handset is 'simply a platform' and the suggestion that the makers of these devices therefore have no continuing responsibility for anything that might then happen on them. Indeed, the whole idea underpinning the UK code on mobile content and the EU-wide code that has now also been produced⁹⁴ is that precisely because these devices are so portable, they are different and cannot be judged by the same standards as 'conventional' computers. The range of features packed into the mobile phone handsets not only adds to their attractiveness to many young people, they also increase the number of risks associated with them.

⁹³ Shipments of wifi-enabled mobile phone handsets are set to double in volume by the end of 2010, and a similar rate of growth will be maintained up to 2013. See www.abiresearch.com/press/1370-Dual-Mode+Cellular_Wi-Fi+Handset+Shipments+to+Double+from+2008+through+2010

⁹⁴ www.gsmworld.com/newsroom/press-releases/2008/871.htm

The mobile phone handset manufacturers actively promote and glamorise their new handsets to children and young people, so they must accept a larger role and take more responsibility in the ongoing discussions about child safety on the internet as well as within the wider digital environment.

Notwithstanding that there remain serious issues to be resolved around precisely how dangerous mobile phone handsets can be if used by very young children,⁹⁵ it is plain that many millions of parents are buying mobiles for their children aged 11 and under, if only to help with communications within the family. In that light, and particularly for this younger group, CHIS can see a strong case for the phone manufacturers and the networks to consider developing products that are specifically tailored towards the needs of this group.⁹⁶

Mobile phone handset manufacturers and network providers should consider developing devices for children that have a much-reduced feature set and therefore avoid some of the risks that seem to be unavoidably associated with the more sophisticated models.

Major providers of wifi access should replicate the arrangements currently made by the mobile phone companies for restricting access to adult sites on the internet.

The mobile phone handset manufacturers should accept a larger role in the ongoing discussions about child safety on the internet with a view to developing safety features that can operate by default and are integrated directly into the handsets.

⁹⁵ www.iegmpgorg.uk

⁹⁶ This does not mean that CHIS favours any relaxation of the rules on advertising to children and young people. They should still apply irrespective of what is being sold.

Advertising

It has been estimated that children and young people between the ages of seven and 19 spend around £12 billion per annum from their pocket money or from the proceeds of part-time jobs.⁹⁷ This is a substantial market in its own right but it has been calculated that, when you take into account what parents also spend on their children, and the degree of influence many children have over such expenditure, the size of the children and young people's market balloons to an astonishing £99 billion.⁹⁸

CHIS has considerable concerns about the level and nature of advertising to children. The internet should not be a route for advertisers simply to avoid restrictions on advertising to children and young people that apply in all the other media. Under the long-established rules of the Advertising Standards Authority (ASA), it should always be easy to distinguish between material that is presented as being factual and material that is intended to advertise or promote a product or service. On the internet, the line is too often and too easily blurred. This is completely unacceptable in relation to children and young people, who will typically be far less skilled at discerning the differences and therefore be far more open to manipulation by the seller. For example, the role of 'adver-games' is particularly problematic. These are games where, at different points in the play, the child is encouraged to buy something from the game provider's inventory, perhaps to decorate their website, speed up their progress in the game or help them succeed more easily within it.

⁹⁷ www.tgisurveys.com/tgi/youth2006.pdf

⁹⁸ Estimates by Ed Mayo and Agnes Nairn in *Consumer Kids*, Constable and Robinson, January 2009.

It could be argued that every company's website is, to some degree or other, a form of advertising and therefore broadly speaking everything that appears on it should be classed as and governed by the rules of advertising.⁹⁹

The Byron Review made two specific recommendations about advertising:

1. That the advertising industries take steps to 'futureproof' the current system for regulating advertising to take account of new forms of online advertising that are currently out of remit, and that Government reviews progress in this area in a year's time, when it has the conclusions of the assessment of the impact of the commercial world on children's wellbeing.¹⁰⁰
2. That the advertising industry works with media owners to raise awareness among advertisers of their obligations under the CAP Code to advertise responsibly to those under 18 on the internet.¹⁰¹

At the time of writing, the ASA is about to publish its response to the Byron recommendations. It will clearly be very important for the UKCCIS Executive Board to give close and careful consideration to the ASA's report.

Some of the issues lying behind Byron's concerns have arisen from studies that have documented¹⁰² many instances of wholly inappropriate advertisements appearing on websites that are predominantly aimed at or are exclusively for children and young people,

for example advertisements for products or services that children and young people could not legally buy, such as alcohol or gambling.

Drawing on a parallel practice used to determine where it is permissible for gambling companies to advertise, *Consumer Focus* has suggested that any website where 25% or more of the regular visitors are under the age of 18, or where 100,000 or more regular visitors are children and young people under the age of 18, should be considered to be a children and young person's site and the rules about advertising on that site should be framed accordingly.¹⁰³ CHIS endorses this view.

A clear definition of what constitutes a children's website should be formulated and all advertising on such sites must conform to the ASA's Code of Advertising, Sales Promotion and Direct Marketing (CAP code).

CHIS very much hopes that, in its response to the Byron Report, the ASA will also express a clear view on the recruitment of children to market toys or other products virally over the internet. Online peer marketing is a contentious issue in its own right when only adults are involved. Engaging very young children in it seems to us to be wholly unacceptable.¹⁰⁴

¹⁰³ Also in the letter referred to above from Ed Mayo, CEO of Consumer Focus, to the COO of the Advertising Association, October 2008.

¹⁰⁴ Although it is accepted that properly conducted market research among and involving children, and product testing by children and young people, are perfectly legitimate activities if conducted within a clear ethical framework.

⁹⁹ Letter from Ed Mayo, CEO of Consumer Focus, to the COO of the Advertising Association, October 2008.

¹⁰⁰ The Buckingham Report. At the time of writing, its publication date is still uncertain.

¹⁰¹ Ibid, Executive Summary, para 16

¹⁰² Eg *Fair Game: Assessing commercial activity on children's favourite websites and online environments*, National Consumer Council and Childnet International, December 2007, <http://kidnet-int.org/downloads/fair-game-final.pdf>



Part 2: Ongoing concerns

Child safety software

Typically, a child safety package will allow a parent to set age-appropriate limits on how a child or young person might interact with the internet. The software can help a parent, or a school, to screen out unwanted content from the internet, for example pornography or violent images. It can restrict the times at which a child might access the internet, and it can also restrict the types of websites or other parts of the internet that a child might access. CHIS considers that all devices or connectivity packages that provide internet access in the consumer market should come with child safety software pre-installed and set to a high level of security. Mobile phone companies have shown the way in this respect. ISPs and other companies selling internet-enabled devices should do the same.

No child safety software package is perfect and it is therefore important that parents and teachers retain a close interest and involvement in how their children use the internet. However, these safety packages have become even better and more reliable in recent years. There is no doubt they can provide an important level of protection. They can be particularly useful in busy households with younger children, or households with young people who may have certain vulnerabilities, whether these are permanent or short term.

A parent can customise the operations of this type of safety software to meet the specific needs of their child or children. If parents, carers or other adults working with children wish to liberalise the settings, rather than using the default settings, they should, of course, be able to do so. The criteria used for any default blocking should always be clear

and transparent. However, as things stand currently, few devices are preconfigured with safety software and responsibility for set up is left entirely to parents, carers or other adults working with children.

The rate of take up and implementation of safety software has been disappointingly low but the reasons for this are well known and documented.¹⁰⁵ The packages are not being used because too many adults are either unaware that they are there in the first place, or are worried that if they start changing their computer's settings they will inevitably break the machine and it may be expensive and difficult to fix or be out of action for a long time.¹⁰⁶ This suggests a lack of appropriate support for consumers that the industry needs to tackle and it was one of the key reasons why the British Standards Institute became engaged in this area.

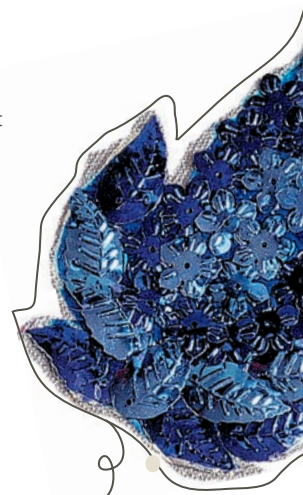
The British Standards Institute¹⁰⁷ recently launched its kitemark for child safety software. The aim is to encourage parents to use safety software by helping them to recognise which products will be most effective and easiest to use.¹⁰⁸ To obtain the BSI kitemark, the software has to meet basic criteria – it has to be easy to use, reliable, and offer parents the support and information they need. There is now an EU project underway to establish a European Standard kitemark for child safety software, thus indicating a much wider level of interest in this idea.

¹⁰⁵ *UK Kids Go Online*, Sonia Livingstone, <http://kidnet-int.org/downloads/fair-game-final.pdf>

¹⁰⁶ When discussing analogous issues, in their report on 'Personal Internet Security', 5th Report of Session 2006–07, the House of Lords Science and Technology Select Committee said it was 'no longer realistic' to leave responsibility for personal internet security entirely in the hands of the individual. The Committee called for a robust and vigorous new approach that, in the end, may require 'direct regulation'.

¹⁰⁷ With support from the Home Office and OFCOM

¹⁰⁸ www.bsi-global.com/en/ProductServices/Kitemark-for-Child-Safety-Online





One of the arguments most frequently advanced against setting safety software on a device by default is that it will induce in parents a false sense of security. It is suggested that if software is installed, parents will think that safety issues have been adequately addressed and they will not take an ongoing interest in their children's internet use. In contrast, the alternative view is that if properly implemented, the pre-installation and pre-configuring of this software can help enormously with engaging parents with these issues.

The Government should announce that within the next 12 months it intends to begin a review of progress on the take up and use of child safety software in the consumer market in respect of all internet enabled devices.

The Government should consider providing incentives for firms to develop new ways of protecting children and young people online.

Training needs for professionals

The Byron Review's terms of reference did not allow Professor Byron to look at how the staff in the National Offender Management Service (NOMS), principally the probation and prison services, seek to safeguard children by ensuring that sex offenders or those with problematic behaviour receive appropriate help, treatment or supervision. The social work profession and several other parts of the children's workforce also have an absolutely critical role to play in this area yet they too were not covered by the Byron Review's terms of reference.

The professional bodies responsible for the accreditation of police, health, probation, prison staff, social workers, youth workers and teachers need to ensure that proper recognition is given within their professional qualifications and their professional development programmes to the importance of dealing appropriately with online offending or other related problematic behaviours.

The Ministry of Justice, the Home Office, the Department of Health and other relevant agencies need to ensure that there is sufficient availability and take up treatment programmes for internet offenders. They also need to ensure that police and probation officers are appropriately trained to manage the risks posed by internet offenders, thereby minimising or reducing the prospect of them re-offending or otherwise putting children in jeopardy.¹⁰⁹

There is also a need to ensure that all parts of the judiciary have a good understanding of internet offending. Appropriate advice should be made available to all parts of the judiciary in relation to the nature and impact of the different types of online offending against children and young people.

Responding to children who are sexually harming online

While some young people will choose to explore issues in relation to their sexuality and sexual behaviour via the internet, it is important to recognise that this exploration may sometimes lead to other children and young people being harmed.

It is also important that there is an appropriate response to such abusive incidents. This response should challenge the behaviour of the child or young person but should not seek to criminalise them. For children under the age of 18 who sexually abuse or harass other children using the new technologies, the child protection system should be the preferred route of intervention, not the criminal justice system.

¹⁰⁹ As a recent pilot involving the Lucy Faithful Foundation has shown, some of the most successful ways of managing internet offenders can make effective use of the technology itself: see www.securus-software.com/pdf/monitoringoffenders.pdf



Appropriate assessment and treatment should be available for children displaying inappropriate or aggressive sexual behaviour online.

It is important that we develop a better understanding of the range and spectrum of children's sexual behaviours online and develop a better understanding of how to assess and treat harmful sexual behaviours that are manifested in the online environment.

In the USA, there have been several well-publicised cases where minors have been prosecuted for posting sexual images of themselves. Not being privy to all the facts it is difficult to give a definitive view of such cases but branding a child a criminal is very unlikely to help get them the right kind of help and support. There have been reports of similar cases in the UK. None have led to a prosecution although, clearly, this kind of behaviour can expose a child to a number of potential harms both now and in the future. Under the United Nations Convention on the Rights of the Child (UNCRC), the use of criminal sanctions should always and very clearly be a measure of last resort in relation to children under 18.

Standards for social networking sites

In February 2008, one of the last acts of the former Home Office Task Force was to publish a guidance note entitled 'Good practice guidance for providers of social networking and other user interactive services'.¹¹⁰ A year later, in February 2009, the EU published a similar self-regulatory guide for social networking sites across all EU member states that was broadly similar to the UK document.¹¹¹

It is not acceptable to CHIS that some major social networking sites continue either to have no means to review and remove harmful content proactively or they refuse to accept they have any responsibility to undertake this role. To justify their position, they point to the EU's E-Commerce Directive, which confers 'mere conduit' status on ISPs and other types of online service providers. CHIS would like to see every social networking site give a clear commitment to setting up measures for proactively reviewing content. The argument that this is technically not feasible is no longer convincing – some sites do it, all sites should do it.

Efforts should be made to clarify the civil and criminal liabilities of ISPs and other online service providers in relation to user-generated content hosted on their websites. In particular, the Government should press for an amendment to the E-Commerce Directive to remove any disincentive for internet companies to police their own sites for fear of attracting liability. ISPs and other online hosting companies should not lose the protection of 'mere conduit' status simply because they sought to police their site to locate or remove inappropriate or illegal content. The principle should be that, for liability to exist, it is necessary to show that an ISP or hosting company had actual knowledge of the content and deliberately took no action.

CHIS also considers it is unacceptable that some sites still have no clear mechanisms for children to report problems, as this can be a starting point for children getting help. In addition, CHIS is concerned about the unresponsiveness of some social networking sites to complaints or issues raised by the public,¹¹² and even a lack of flexibility in relation to quite delicate issues of child protection.

¹¹⁰ <http://police.homeoffice.gov.uk/publications/operational-policing/social-networking-guidance/>

¹¹¹ 'Safer Social Networking Principles for the EU', http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf

¹¹² An observation also made by the House of Commons Select Committee on Culture Media and Sports: see www.publications.parliament.uk/pa/cm200708/cmselect/cmcmmeds/353/35302.htm

An example of this that CHIS became aware of was in an adoption case where the birth parent attempted to contact a child who had been entrusted to the permanent care of another family. The birth parent tried to make contact by posting a request for information about the child's whereabouts. The site where the request was posted insisted that the adoptive parents had to raise the matter with them directly. The site refused to respond to an intercession by the adopting agency that had placed the child. It should be possible for sites to respond to reports or requests received from trusted third parties, for example an adoption agency or a recognised child protection agency acting in good faith, rather than insisting that the adoptive parents identify themselves. That could compromise the child's anonymity, and with it the child's security. This example reflects poorly on the flexibility, responsiveness or even understanding and interest in child protection issues of those running such sites.

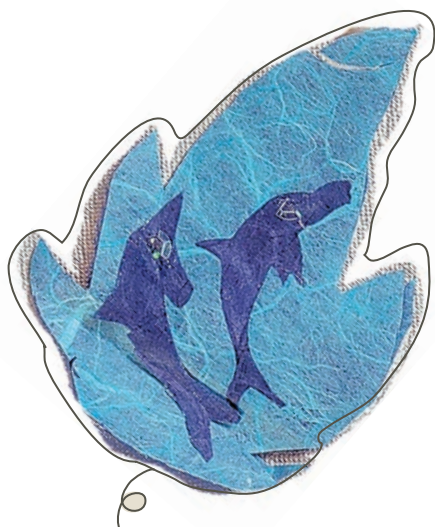
One of the first tasks of the new UKCCIS is to consider how to ensure, through a process of independent review, that the commitments that the social networking sites agreed to when negotiating the Home Office guidance on user-generated content, or whatever replaces it, in fact are being implemented in practice. CHIS thinks this is an extremely important undertaking that ought to proceed with some urgency.



Social networking sites should ensure they meet all the recommendations of the Home Office guidance on user-interactive services, giving urgent attention to their report abuse procedures.

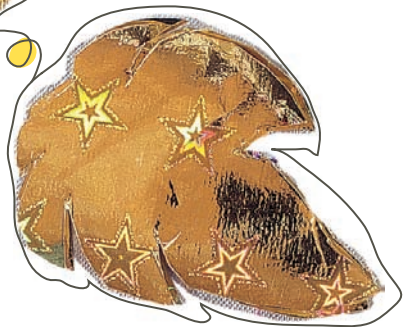
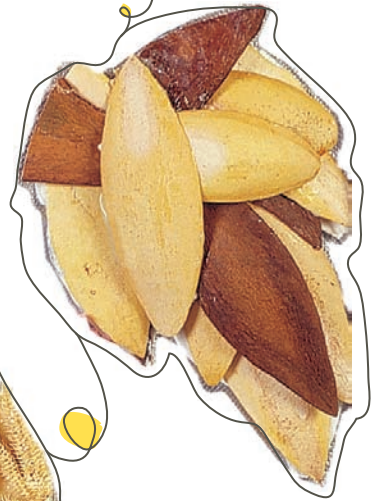
Social networking sites should ensure they have a mechanism that allows them proactively to review content on their site, especially pictures and videos, and also ensure that they review all content reported to them within a clearly specified time period.

UKCCIS should give a high priority to the development of an independent mechanism for determining compliance with the recommendations of the Home Office good practice guidance for the providers of social networking and other interactive services.





Section 6



as long as it takes

Section 6

Self-regulation

The history of self-regulation

In the mid-1990s, when the first cases of online child abuse images started to be reported in the media, the Government and the police were uncertain how to address them. There was little or no knowledge of how the internet worked within the relevant police and governmental circles, and both had to rely very much on the goodwill of the internet industry to interpret and deal with events as they unfurled.¹¹³

Thus self-regulation in the internet space was born out of a practical necessity. It most emphatically was not a careful choice made from among a range of available options, although self-regulation and ‘light touch regulation’ were very much the order of the day with the then Conservative Government.

In April 2001, the by now Labour Government announced the formation of the Home Secretary’s Internet Task Force on Child Protection to take on a broader range of issues. The Task Force fully embraced the self-regulatory principle. Its aim was to address some of the most serious child protection concerns related to the internet and to come up with solutions that, as far as possible, did not require legislation. The codes of practice referred to earlier¹¹⁴ were the main output of the Task Force. However, there were in fact a number of instances where it was agreed that changes in the law were necessary, for example in relation to the offence of grooming, but otherwise (with rare exceptions)¹¹⁵ it was widely accepted that progress could best be made through agreeing and making changes in practice that did not require changes in the law.

¹¹³ The creation of the IWF in 1996 was one of the first fruits of this new relationship.

¹¹⁴ See above pg 23

¹¹⁵ The best known, perhaps, being over granting to the police powers to require decryption keys, contained in the Regulation of Investigatory Powers Act, 2000.

Does self-regulation have a future?

The established consensus around the idea of self-regulation was reflected in the Byron Report. Undoubtedly, self-regulation has produced many benefits in the past, but is it possible it may no longer be fit for purpose?

The rate of technological change, and the rate of take up of technology by children and young people, are both quickening. Some of the protracted processes involved in the consensus-building approach of the self-regulatory model can mean, in effect, the pace at which things happen is determined by those least willing to engage in and support the process.

The way in which the new breed of location services have emerged into the UK mass market also indicates how companies can engage, or not engage, with discussions around online child safety according to their own internal perceptions of relevance or risk. The continued absence of the mobile phone handset manufacturers from any of the regular forums where online child safety issues are discussed also speaks to other weaknesses in the approach.

Despite having the technical know-how in place for five years and a public declaration from Government that it wanted the whole of the industry to comply, the UK still does not have 100% coverage in terms of blocking child abuse images. If self-regulation cannot deliver here, where there is complete agreement about the desirability of the objective, what hope is there that it can deliver in other areas of online child protection policy where matters are more contested? It is too easy for the term ‘self-regulation’ to become code for saying to parts of industry ‘Do it if you want to, but if you don’t want to, don’t bother.’

One of the key potential dangers with self-regulation is that the Government and law enforcement can become involved in relationships with industry that, in effect, make them dependent on them to an unhealthy or undesirable degree. When discussing regulatory issues, the industry itself is looked to for advice and information about what is technically possible and what is not technically possible, what can be achieved economically and what cannot be considered because it is disproportionately expensive. In essence the industry is asked how, if at all, it would like to be regulated. Everything becomes a negotiation where the two sides are not equally balanced.

Self-regulation has been the basis of policy in this space in the UK for many years yet levels of public anxiety about the internet have not notably diminished. Can this all be explained by, as many in the industry see it, the constant, hysterical overreaction of the mass media in general and by the tabloids in particular? Such an analysis is far too simplistic.

The UK is now in the 13th year of self-regulation. Self-regulation is beginning to feel like an increasingly fragile vessel. Every stakeholder needs to reflect on what they can do to preserve the model by convincing many of those who are currently unconvinced that things truly are getting better. More than a year on from Byron's recommendations this challenge needs to be posed to the industry, perhaps more starkly than she did in her report.

The Government and law enforcement should seek to reduce their dependency on the internet and high-tech industries by developing their own independent sources of technical knowledge and expertise in these highly complex areas.

The Government should find ways to help the third sector to develop its own capacity to engage constructively and in a well-informed way, both nationally and internationally, with the consultative and other processes that are central to the development of policy in this area.

For public confidence in self-regulation to be sustained, the model must be seen to work effectively. More energetic and visionary leadership from the high-tech industries is required.





Action for Children
Registered Office
85 Highbury Park
London N5 1UD
Telephone: 020 7704 7000
Fax: 020 7226 2537

Action for Children is committed to helping the most vulnerable children and young people in the UK break through injustice, deprivation and inequality, so they can achieve their full potential.

www.actionforchildren.org.uk

as long as it takes